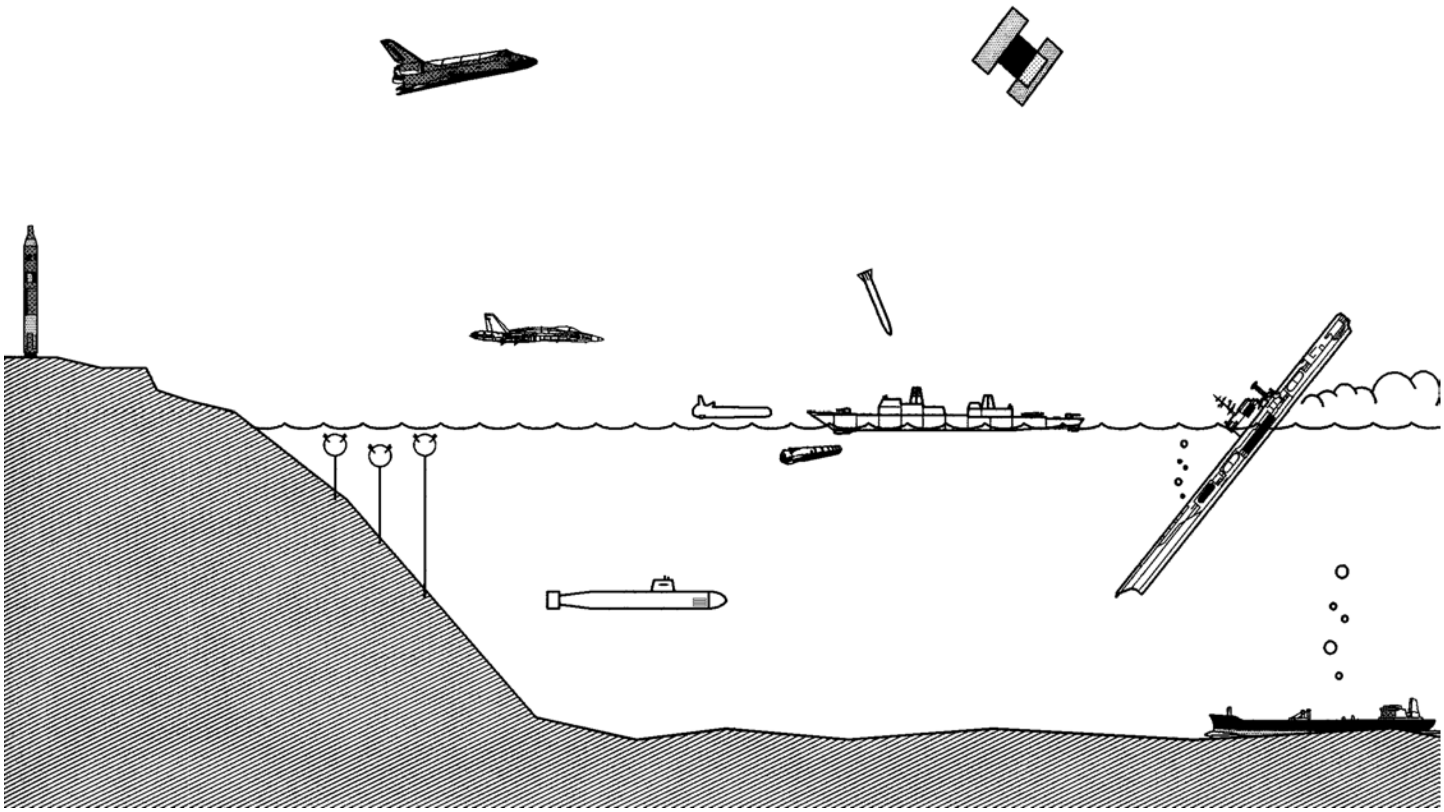
THE ENEMY'S ACCESS DENIAL SYSTEM

POTENTIAL COMPETITOR EXPLOITATION OF U. S. MILITARY VULNERABILITIES



Dr. Robert C. Harney

NPS-JW-01-014

Naval Postgraduate School
(NPS)

The Naval Postgraduate School mission is to increase the combat effectiveness of U. S. and Allied armed forces and enhance the security of the U.S.A. through advanced education and research programs focused on the technical, analytical, and managerial tools needed to confront defense-related challenges.

Institute for Joint Warfare Analysis
(IJWA)

The Institute for Joint Warfare Analysis was founded in 1994 with the mission of addressing the problems of the joint defense arena with the academic disciplines resident at NPS. It sponsors a wide ranging research program, curriculum development focused on joint warfare, and interaction with numerous services and DoD organizations.

Institute of Joint Warfare Analysis
Naval Postgraduate School
Monterey, California, 93943-5000

NPS-JW-01-014

THE ENEMY'S ACCESS DENIAL SYSTEM
POTENTIAL COMPETITOR EXPLOITATION OF U. S. MILITARY VULNERABILITIES

Dr. Robert C. Harney

NAVSEA Chair of
Total Ship Systems Engineering
(Combat Systems)

7 December 2000

Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE 7 December 2000	3. REPORT TYPE AND DATES COVERED Technical
4. TITLE AND SUBTITLE The Enemy's Access Denial System: Potential Competitor Exploitation of U. S. Military Vulnerabilities		5. FUNDING NUMBERS Not Applicable
6. AUTHOR(S) Robert C. Harney		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER NPS-JW-01-014
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) None		10. SPONSORING/ MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES The views expressed in this report are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.		
12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited.		12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

As part of an experimental approach to "red teaming" that is studying the problem of enemy access denial systems, the author performed a detailed investigation of the vulnerabilities of the U. S. military's power projection capabilities. The primary purpose of this document is to facilitate out-of-the-box thinking by future "red teams". Thirty-six separate areas of vulnerability relevant to access denial were identified The vulnerabilities span all ranges from tactical to strategic, from weapons to logistics, and from military to societal. The agreement between this "list" of vulnerabilities and a previous list prepared independently by the Defense Science Board is striking. There is additional strong support for this list in the specific weapons systems that the three different "red teams" involved in the access denial study (all of whom preceded the completion of this study) opted to develop for their 2020 epoch force structures.

Each of the 36 vulnerabilities identified here is examined in detail to define the nature of that vulnerability, its causes, and the things that affect it. In addition, specific ways in which a potential "near peer competitor" could exploit those vulnerabilities to enhance his access denial capability are discussed. In addition to it future use in "red teaming", it is expected that this analysis can aid:

- U. S. military staff in their long-range planning activities,
- the military R&D community in determining areas that need additional research, and
- intelligence professionals in identifying out foreign activities that might indicate a competitor's intent to create an access denial capability.

It can also be used as a starting point for other vulnerability studies.

14. SUBJECT TERMS Vulnerability, Access Denial, Force Projection, Threat, Cruise Missiles, Ballistic Missiles, Submarines, Mines, Weapons of Mass Destruction, Special Operations, Sealift, Airlift, Basing, Pre-positioned Equipment, Logistics, Intelligence, Surveillance, Disruptive Technologies			15. NUMBER OF PAGES 426
			16. PRICE CODE
17. SECURITY CLASSIFICATION - REPORT Unclassified	18. SECURITY CLASSIFICATION - THIS PAGE Unclassified	19. SECURITY CLASSIFICATION – ABSTRACT Unclassified	20. LIMITATION – ABSTRACT UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

TABLE OF CONTENTS

SUMMARY

INTRODUCTION

As part of an experimental approach to "red teaming" that is studying the problem of enemy access denial systems, the author performed a detailed investigation of the vulnerabilities of the U. S. military's power projection capabilities, as they are likely to exist in the year 2020. The primary purpose of this document is to facilitate out-of-the-box thinking by future "red teams". Thirty-six separate areas of vulnerability relevant to access denial were identified, including:

Attacks Using WMD:	Attack by Nuclear Missiles (ICBMs) Attack by Other Weapons of Mass Destruction
Direct Attacks Against Forces:	Attack by Cruise Missiles Attack by Ballistic Missiles or Superguns Attack by Transatmospheric Aircraft Attack by Naval Mines Attack by Advanced Torpedoes Attack by Advanced Non-nuclear Submarines Attack by Unmanned Air Superiority Vehicles Attack by Infrared Anti-Aircraft Missiles
Counters to Offensive Systems:	Reliance on Stealth Jamming of GPS & GPS-Dependent Systems Jamming of Precision-Guided Weapons
Attacks on C4I Assets:	Attack by Electromagnetic Weapons Attack by High-Energy Lasers Attack by Information Warfare Attack by Antisatellite Weapons Reliance on Long-Range Airborne Surveillance Susceptibility to Strategic Deception Excessive Intelligence-Response Latency
Unconventional Methods of Attack:	Attack by Special Operations Forces Limited Adverse Weather Operations Capability Attack by Nonlethal Weapons
Attacks on Logistics Resources:	Limited Strategic Sea/Air Lift Capability Reliance on Limited Overseas Basing Reliance on Pre-Positioned Equipment Reliance on Underway Replenishment
Attacks on Societal Vulnerabilities:	Civilian Intolerance of Casualties Restrictive Rules of Engagement Civilian Intolerance of Unnecessary Hardships Need for Coalition Support Unequal Societal Transparency Treaty Limitations
Technological Change:	Technological Surprise Technological Atrophy Disruptive Technologies

The following paragraphs give a brief description of each of these identified vulnerabilities. Detailed descriptions and associated analyses can be found in the main body of the paper.

VULNERABILITIES

Attacks Using WMD – Even if the United States develops and deploys a National Missile Defense system, it will only defend against a small number of ICBM threats. We will remain vulnerable to those powers possessing enough nuclear weapons and delivery systems to overpower that defense. The ability of certain adversaries to hold us hostage in a mutual assured destruction sense has and will continue to have a profound influence on our policies and military options.

The United States is profoundly vulnerable to attacks by other forms of WMD, especially chemical and biological weapons. Only military forces have minimal defenses against chemical and biological (CB) weapons. Even these defenses cannot hold up for many days, if an adversary were to employ chemical or biological weapons on a massive and protracted basis. Current U. S. naval forces are capable of surviving CB weapon attacks but must immediately evacuate the contamination zone for decontamination. They cannot stay for extended periods and fight. The U. S. homeland is virtually undefended and indefensible against CB weapons. Terrorist employment is a likely scenario. CB weapons employed on a large scale against U. S. logistics facilities could delay power projection forces for weeks, allowing an adversary more time to prepare or even create a *fait accompli* for the U. S. to counter.

Direct Attacks Against Forces – The sinking or severe damage to several warships by cruise missiles in the Persian Gulf and during the Falkland Islands War has made everyone aware of the magnitude of this threat. Although defensive weapons have improved to where limited attacks can be effectively countered, recent studies have suggested that potential adversaries may opt for massive attacks. Any serious adversary can easily afford to buy thousands of inexpensive missiles. In any littoral engagement, such an adversary can easily and repeatedly attack a battle force with more missiles than the defensive systems are capable of destroying.

Many potential adversaries are procuring ballistic missiles with ranges from hundreds to thousands of kilometers. Some are developing terminal guidance systems for these missiles. With adequate targeting information, such terminally guided ballistic missiles are capable of sinking groups of warships at sea. Planned theater missile defense systems may be unable to intercept such threats.

In the changing world economy, the U. S. is not guaranteed to maintain its superiority in aircraft and spacecraft. Should an adversary develop transatmospheric aircraft before the U. S., that adversary will not only take a commanding lead in controlling space, but it will also possess platforms that will be difficult to defend against, yet can deliver surgical strikes against any point on earth at short notice.

Mine warfare has long been one of the weakest of U. S. naval warfare capabilities. An adversary can employ mines to attrit, delay, or divert U. S. naval forces almost at will. With mines being among the cheapest of ship-killing weapons, we can be use any adversary will deploy them in large quantities.

Modern torpedoes are capable of being fired at distances of more than 100 km, tracking down targets by their wake turbulence, and outrunning even the fastest warship. U. S. warships lack adequate defenses against these new torpedoes. Large fleets of coastal diesel submarines, high-speed patrol torpedo boats, or maritime patrol aircraft armed with the latest torpedoes would be capable of inflicting significant damage against any naval force that came within range.

Non-nuclear submarines have significant noise advantages over nuclear-powered submarines. Advanced air-independent propulsion systems promise to free non-nuclear submarines from daily surfacing or snorkeling to recharge batteries. Given the increased submerged range guaranteed by such developments, advanced submarines may be able to track, target, and destroy even the best nuclear submarines, whether in shallow littoral waters or not. U. S. superiority in submarine warfare could well in jeopardy.

Manned fighter aircraft are limited to maneuvers less than 10 g's. An adversary that develops an unmanned air superiority vehicle (UASV) capability will have no such limitations. Unmanned "fighters" with 30-g maneuver capability will literally be able to fly circles around the best modern manned fighters and to outmaneuver current generations of anti-aircraft missiles. Remotely piloted UASVs are possible with today's technology. Within a few years advances in artificial intelligence may permit replacement of the remote pilots.

Stealth technology applied to aircraft promises to reduce the effectiveness of radar-guided anti-aircraft missiles. Current advances in multicolor imaging infrared missiles should prove easily capable of compensating for this loss of radar-guided capability. Not only will such missiles be virtually immune to decoys and jamming, they will be little affected by current stealth technologies, and they will not only be capable of autonomously identifying targets from non-targets at moderate ranges, they may be capable of identifying friendly aircraft from hostile aircraft. If an adversary develops and deploys such missiles, all of our aircraft will become vulnerable to attack, even if initial detection assets are unable to provide fire control solutions adequate for radar-guided missiles.

Counters to Offensive Systems – Stealth has long been considered to be an aspect of U. S. military superiority. Almost every new platform incorporates high levels of stealth, but at the expense of less defensive weaponry, decreased or limited armor, and vastly increased costs (invariably resulting in fewer platforms being purchased). As soon as a major adversary develops and deploys counterstealth sensor capabilities, stealth platforms will be at risk, and may prove unable to accomplish their intended missions. Over-reliance on stealth will change from an asset to a catastrophe.

The same statements can be made about reliance on GPS. The U. S. is making GPS guidance a major feature of new weapon systems and reducing investment in terminal guidance sensors. However, GPS can be jammed, and even improved systems will still be capable of being jammed. If an adversary devotes even a fraction of his electronic warfare assets to denying the U. S. unhindered use of GPS for weapons guidance and navigation, critical strike weapons will not hit their intended targets and a major aspect of U. S. power projection strategy will be nullified.

Another U. S. strength is its capability to employ precision-guided weapons, permitting even critical targets to be destroyed with limited expenditure of ordnance. However, all forms of precision-guided weapons can be jammed. An adversary that invests in such jammers can deny the U. S. ability to effectively use its huge investment in precision-guided weapons. Once again, a perceived strength could be converted to a liability.

Attacks on C^4I Assets – Although most military systems are supposed to be hardened against nuclear electromagnetic pulse, the actual degree of hardness achieved is questionable. Use of a single nuclear weapon to produce localized EMP over the theater of conflict would likely render many of our systems inoperative. Because of their higher frequencies, U. S. systems will be even more vulnerable to non-nuclear electromagnetic weapons such as high-power microwaves. Civilian systems that were designed with no hardening requirements are extremely vulnerable to attack. Terrorist or special operations groups could easily deliver such attacks.

U. S. weapons and systems have limited defenses against high-energy laser weapons. For the same reasons the U. S. is developing this technology (ballistic missile defense, cruise missile defense, anti-satellite weapons), any near peer competitor will attempt to acquire such weapons. If they are successful, then almost any U. S. airborne or spaceborne asset (aircraft, missile, satellite, or spacecraft) will be at risk of immediate, instantaneous, and overwhelming attack.

The U. S. military and indeed the entire infrastructure and economy of the U. S. is dependent on computer networks and the information they contain. Since even a single hacker is capable of accessing critical computer systems (causing loss of data, corruption of data, or crashing of the system), the potential of an adversary army of information warriors to exploit our computer dependence is truly staggering.

Of all the world's militaries, the U. S. is the most dependent on space assets. Weather support, navigation, communications, overhead reconnaissance, and even weapon guidance all depend on satellites. Should an adversary develop anti-satellite weapons based on existing technologies, that adversary could deny the U. S. the use of any or all of these satellite functions at the most critical times. The impact on U. S. military capabilities would be staggering.

U. S. battle planning and operational conduct place significant importance on long-range airborne surveillance assets such as JSTARS, AWACS, and E-2C Hawkeyes. There are limited numbers of these platforms in our inventory and fewer still available to any one theater of operations. If an adversary were to specifically target these assets with sufficient force, they can be destroyed. This would eliminate critical intelligence needed to coordinate ground operations and would make it impossible to conduct efficient air defenses or to coordinate air operations.

The U. S. intelligence services have become overly dependent on technical means such as satellites and communications interception and decryption. The severely limited human intelligence and on-site inspection opportunities afforded by some potential adversaries leaves us open to strategic deception operations. Critical technology developments, facilities, test sites, and even military forces can be completely hidden by determined adversaries in massive underground facilities or disguised as something else entirely. Any attack on such adversaries will undoubtedly result in numerous unpleasant surprises for U. S. forces.

The United States possesses tremendous intelligence capabilities in its satellites and signals intelligence assets. Unfortunately, it takes for any information to be collected, processed, analyzed, and disseminated to those who need that information for tactical purposes. Once received additional delays result in planning missions, allocating resources, and deploying weapons against the targets. Delays can range from minutes to days. New initiatives may reduce latency but will probably never reduce it to insignificant levels. The excessive intelligence-response latency times can preclude many missions from being efficiently performed, such as "Scud-busting" during the Gulf War. An adversary can take advantage of the latency by maximizing the degree of mobility afforded to certain assets. Ballistic missiles systems that can move from under cover, set up, launch, tear down, and return to different covered hides in periods of a few minutes will be extremely difficult to target, even if they are detected. Similar mobility afforded to air defense sites would make it difficult to plan air missions for minimum attrition.

Unconventional Methods of Attack – The Special Operations Forces (SOF) of the United States military are capable of conducting sabotage, intelligence, and/or surgical strike operations against the military forces, government, or infrastructure of any country, anywhere, anytime. Although U. S. forces and facilities are off-limits except during exercises, U. S. SOF would be as effective in operations against them as they would be in operations against our adversaries. If an adversary creates its own SOF, there is no reason to expect that they would be less effective against U. S. targets. Our military forces and civilian population are too complacent and totally unprepared to defend against such attacks.

As we proceed into the 21st Century, we will learn more and more about weather and the forces that cause it. U. S. forces are unable to operate in adverse weather. Bombs (even laser-guided bombs) cannot be dropped with precision when the targets are obscured by fog. Aircraft cannot fly safely through severe storms. Surface ships sail hundreds of miles out of their way to avoid the hazards of sailing through tropical cyclones. If an adversary has better knowledge of the weather than the U. S., he can plan his operations so that weather provides the maximum limitation to U. S. forces and the minimum impact on adversary forces. At some point in the next century, it will likely become possible to control the weather. If an adversary gains this capability before we do, he can devastate our economy, damage our infrastructure, and hinder our forces.

Nonlethal weapons pose a special problem because we have neither a firm policy on how to respond to their use, nor defenses tailored to defeat these weapons. Enemy employment of nonlethal weapons is most likely to be used by "civilian" forces as a delaying tactic to permit accomplishment of military operations in other area. Their employment is more likely during times of crisis that have not escalated to open hostilities. The U. S. lacks response options other than use of lethal force, alteration of course (probably ineffective), or withdrawal. On-scene commanders will be forced to either take actions that will minimize the delay but may make them war criminals, or to refer the problem to higher command, adding to the delay that is the primary objective of the adversary.

Attacks on Logistics Resources – The United States has a very limited number of aircraft and ships that it can use to perform airlift and sealift functions. Should an adversary attack and destroy these assets or their support facilities, the U. S. would be unable to transport follow-on forces and equipment to the operational theater in a timely fashion. This would leave the rapid deployment forces to carry on the war by themselves for periods far longer than intended.

Concurrent with the downsizing of the U. S. military, the U. S. has reduced the number of overseas bases at which it maintains forward-deployed forces. A number of nations have limited U. S. use of their ports and airfields for military purposes. Without bases close to a region of conflict, the U. S. is unable to marry-up Marine and Army forces with maritime pre-positioned equipment. We are also unable take advantage of shortened logistic supply lines. Our weakness in this area would be exacerbated if an adversary were to take active measures (such as direct attack) against the few remaining U. S. forward bases.

Because we have inadequate sealift and airlift capabilities, the U. S. has opted to pre-position large quantities of military equipment and supplies near regions of anticipated future conflicts. This equipment represents almost all of the equipment available for the first wave of follow-on forces. Centralized in a few weakly defended locations, this pre-positioned equipment is a logical target for pre-emptive strike by an adversary. Destruction of this equipment would delay arrival of effective follow-on forces for many weeks.

U. S. naval forces carry limited amounts of food, fuel, and ammunition. In combat it is expected that ships would be regularly replenished at sea by dedicated ammunition ships and oilers. The U. S. possesses only a limited number of such combat support ships. These ships often sail unescorted over long distances between resupply ports and the combat operating areas. If an adversary were to selectively target the replenishment ships, it could cripple U. S. ability to conduct naval operations. Lacking the specialized "unrep" equipment, conventional cargo ships or tankers used as alternates would be highly inefficient at best, even if they could be readily obtained.

Attacks on Societal Vulnerabilities – The U. S. public has shown a high degree of intolerance of casualties in U. S. military operations. Many senior military commanders have even less tolerance. If an adversary can demonstrate the ability to inflict large numbers of casualties on U. S. forces early in any engagement, those casualties may cause U. S. forces to withdraw or to pursue other tactics. Commanders will try to prevent provoking the sort of "Vietnam War" syndrome that turned public support against the military and ultimately forced U. S. withdrawal.

The U. S. military operates under "Rules of Engagement" that restrict the operations it can conduct, the weapons it can use, and the targets it can attack. Even in wartime these rules are enforced to prevent fratricide, unnecessary civilian casualties, and attacks against neutrals and non-combatants. An adversary can use these rules of engagement against us by collocating military targets with off-limits targets (such as hospitals) or disguising unconventional warfare craft as neutral fishermen or merchantmen.

The U. S. civilian population is intolerant of hardships that they consider unnecessary. Adversary actions that lead to civilian hardships without directly threatening people could lead to erosion of public support for continued conflict. Possible actions include: causing gasoline rationing by disrupting world oil production, limiting public air travel by forcing the U. S. to draft Civilian Reserve Air Fleet assets for airlift purposes, or causing limited food shortages through biological weapon attacks on major food crops.

In recent conflicts the U. S. has been reluctant to act alone. It has desired coalition efforts to mollify world opinion, to foster civilian support for the action, to share the costs of military operations, and to provide additional capabilities that the U. S. military needs. An adversary can take many actions to make forming a coalition harder or to break up or weaken an existing coalition. Should these be successful, the U. S. would be forced to reevaluate its strategic position and ambitions in the region, and possibly withdraw from the conflict.

U. S. society is almost completely transparent to outside observation. Many potential adversaries are closed societies in which it is difficult for outsiders to conduct intelligence operations. The inequality in transparency results in lop-sided flows of technical, economic, and cultural information necessary to predict long-term goals, short-term capabilities, and governmental priorities. Serious adversaries take advantage of the unequal transparency to evaluate their relative capabilities vs. U. S. forces and to acquire the information necessary to reduce and minimize any deficiencies they uncover.

The U. S. is a signatory to many bilateral and multi-lateral diplomatic agreements (treaties, protocols, etc.) that significantly restrict military options for responding to crisis situations. Some of these treaties create vulnerabilities. For example, the ABM Treaty prohibits testing of ballistic missile defense systems against targets missiles with ranges and velocities well below those of ICBMs, yet well within the range of practical construction. If an adversary deployed antiship warheads on such longer-range missiles, we could never assure ourselves that our deployed defenses would actually work in combat, without violating the treaty.

Technological Change

No country today can be the leader in every field of technology development. However, it is important to be a credible player in every field. Failure to do so can lead to technological surprise. If an adversary develops a critical technology and can keep it secret, then that adversary has a significant window of relative superiority that it can exploit. It is considerably more difficult to effect a significant degree of surprise, if both sides have roughly comparable levels of expertise in a subject. In addition, the duration of any window of vulnerability will certainly be shorter, if the surprised party is only a short way behind the surprising party in the relevant technology. The U. S. will become more vulnerable to technological surprise as it relinquishes it leadership in more and more technologies (a trend that also creates a second distinct form of vulnerability).

The technological superiority that kept the U. S. a superpower during much of the 20th Century is in danger of disappearing. Complacency, poor policy decisions, deteriorating educational systems, and the lack of a national vision of the future, to name a few of the factors, have combined to produce conditions where our national technological might may begin to atrophy. If things decay to a state where other countries are developing the cutting edge weapons, then our military will no longer have the technological force multipliers. Loss of these multipliers coupled with our diminished manpower may mean we are unable to fight and win those battles deemed critical to our national security.

"Disruptive technologies" are technologies that completely disrupt the status quo. They may be slow to develop. They may have little impact as they become established, except in niche areas, but they have the potential to change almost every aspect of how wars are fought. For example, the tank, once its function had been truly appreciated, transformed land warfare from "attrition warfare" (defense-oriented trench warfare) to "maneuver warfare" (offense-oriented blitzkrieg). U. S. military forces invest so much effort and capital in expensive yet evolutionary high technology equipment and extensive doctrine and training at all levels in the use of that equipment, that they often cannot respond quickly when disrupting technologies arise. Potential adversaries that are quicker to adapt to disrupting technologies can exploit that potential vulnerability in U. S. forces.

ANALYSIS AND CONCLUSIONS

The vulnerabilities described above span all ranges from tactical to strategic, from weapons to logistics, and from military to societal. The agreement between this "list" of vulnerabilities and a previous list prepared independently by the Defense Science Board is striking. There is additional strong support for this list in the specific weapons systems that the three different "red teams" involved in the access denial study (all of whom preceded the completion of this study) opted to develop for their 2020 epoch force structures.

Each of the 36 vulnerabilities identified here is examined in detail to define the nature of that vulnerability, its causes, and the things that affect it. In addition, specific ways in which a potential "near peer competitor" could exploit those vulnerabilities to enhance his access denial capability are discussed. In addition to it future use in "red teaming", it is expected that this analysis can aid:

- U. S. military staff in their long-range planning activities,
- the military R&D community in determining areas that need additional research, and
- intelligence professionals in identifying out foreign activities that might indicate a competitor's intent to create an access denial capability.

It can also be used as a starting point for other vulnerability studies.

If the reader is willing to accept various technical assertions on faith, then reading the main body of the paper will suffice. The analyses of vulnerabilities presented therein are basically non-technical in nature. However, for those who question some of the technical assertions, or those who need more explanation of a subject, a number of technical notes and technical appendices are included which elaborate on the more technical aspects of the analysis. These are designed for the reader with a limited degree of technical training, but an advanced degree is not required. Included are discussions of weapons of mass destruction, radar performance analysis, ballistic missile defense, stealth, missile guidance, directed energy weapons, and nonlethal weapons, among others.

CHAPTER 1. INTRODUCTION – THE AREA DENIAL STUDY

The cornerstone of United States political/military foreign policy rests on an almost undisputed ability to project military power on short notice to virtually any corner of the world. The four pillars on which our power projection capability is based are [1]:

1) Capable, forward-deployed forces in regions of probable conflict,
2) Pre-positioned equipment and supplies in or near potential conflict areas,
3) Pre-positioned equipment afloat, and
4) Rapid transportation of air, land, and sea forces from CONUS and other theaters.

Whenever trouble of any kind arises overseas, our first response is to move one or more forward-deployed aircraft carrier battle groups (CVBGs) to the region to show the flag and demonstrate our national concern. We may also move one or more Marine amphibious ready groups (ARGs) into the region. Should the situation appear to involve imminent hostilities, we may then deploy the 82nd Airborne Division (or a similar light division) and/or a Composite Air Wing to friendly bases in the region. If hostilities escalate, we are then in a position to immediately provide whatever response is warranted. This response can vary from destroying a key facility with a single Tomahawk missile to attacking assembled hostile forces with a massive air strike to blunting a planned invasion with a battalion-sized (or larger) blocking force of Marines or infantry supported by air power. If hostilities begin in earnest, we will move additional personnel and readily mobile assets from their bases in the United States or other theaters to friendly bases where equipment and supplies have been pre-positioned or ports where maritime pre-positioned equipment has been transported and unloaded. These larger and more heavily armed follow-on forces will reinforce the rapid deployment forces already in theater.

This mode of operation has served the United States reasonably well over the last few decades. However, some military strategists have become concerned that our reliance on this mode of power projection to influence foreign policy will lead potential competitors to develop **area denial systems** (or more properly access denial systems) to blunt our ability to project power. If a competitor were successful in developing an access denial system, our ability to influence affairs in that region of the world by any means other than economic ones (trade, loans, investments, etc.) would almost entirely disappear. As we will see, the very pillars of our power projection ability create areas of vulnerability that a potential adversary can exploit to achieve access denial. Given that competition is a constant in world affairs – new competitors will arise whenever old competitors fade away – then the potential rewards of having an access denial system guarantee that one or more potential competitors will try to acquire one.

Because of this, access denial is a topic that is receiving increasing attention at the highest levels of our military [2], [3]. Recently, the term "**anti-access systems**" has begun to replace access denial systems in the lexicon of many military leaders. Given the origin of the present work, we will continue to use the term access denial throughout this report. However, anti-access could be substituted one-for-one for access denial and the meaning and impact would not change in the slightest. Access denial can be defined as **the ability** of competitor military forces **to keep** United States **power projection assets** (carrier battle groups, amphibious ready groups, long-range aviation, and airborne troops) **at sufficient distance** to prevent those assets from inflicting significant damage on the competitor's military forces or civilian infrastructure **for a period of time sufficiently long** for the competitor's objectives to be achieved. As part of almost any access denial strategy, in-theater air, sea, and land bases will be denied to the United States, precluding the gradual buildup of forces which is the cornerstone of current campaign planning. Gradual peeling back of the defenses of the adversary will be made difficult by adversary defensive systems with coverage (range and angle) greater than those of U. S. offensive systems. In short, the United States will be forced to return to a strategy of attrition warfare, and accept the massive casualties that inevitably result, or it will be forced to withdraw and avoid the confrontation.

Had Iraq possessed an access denial capability, the sea, air, and land bases in the Persian Gulf would not have been open to Coalition forces or open only under threat of frequent attack. Bases in Turkey would have become equally hazardous for U. S. forces. There would be no safe havens. The Red Sea, Eastern Mediterranean, and Arabian Sea would have become areas of significant risk for any naval combatant (surface or subsurface). Thus, the lengthy low-risk buildup of Coalition ground forces in Saudi Arabia would not have been possible. Naval forces could not have delivered the massive cruise missile strikes that opened the air war without suffering serious losses. Only long-range bombers and fighters operating from bases in Western Europe (using multiple air-to-air refuelings) could have been used in the air war. These would have faced air defenses that had not been disrupted by attacks on command & control nodes and suppressed by direct attacks as well as air forces that had not been destroyed on the ground. In short the Iraqi annexation of Kuwait could not have been seriously contested by the conventional military means then available if Iraq had possessed an access denial system.

No nation lacking an access denial capability could be considered a true peer competitor to the U. S. or a superpower. It should be noted that throughout the Cold War the conventional military forces of the Soviet Union gave them a sufficient access denial capability that we did not dream of sending any military forces (other than spy submarines) into those "bastions" which the U.S.S.R. declared off-limits. Among these bastions were the Sea of Okhotsk, the Black Sea, the Eastern Baltic Sea, the Barents Sea, and anywhere in Eastern Europe. Except for the traditional diplomatic observation of national sovereignty and non-interference in the affairs of our allies, we accorded the same treatment to no other nation. Indeed when countries like Libya (in the Gulf of Sidra) attempted to establish such off-limits zones, we routinely defied the attempts with lethal results.

The work described below was initiated as part of the NPS Area Denial Study. In 1997 and subsequent years at the request of the Office of Naval Research and the Executive Panel of the Chief of Naval Operations, the Naval Postgraduate School undertook to develop a credible and fully justifiable set of long-term threats (circa 2020). Several teams of students and faculty were assembled, each team representing a different potential 2020 adversary to the United States. Each team had four to five officer students (drawn from each of the four military services and more or less equally split between national security and engineering studies) and one or two faculty advisors (typically highly experienced in the systems engineering, design, development, and manufacture of large-scale defense systems). Over the course of several months, each team proceeded to develop their military force structures in three successive 7-year epochs. In each epoch, the team was given an estimate of the military budget it would have available and a national military strategy. The budgets and strategies were developed by outside teams of expert consultants drawn from industry, academia, and government. Wherever possible, the consultant teams included nationally-recognized economic, political, and intelligence experts on the countries being gamed. The consultant groups were chartered to develop strategies and budgets that represented the groups' best estimates as to the actual future course of events. The only guidance given to the groups was to assume less than benign intentions on the part of the foreign government. Obviously, if a potential adversary decides on peace, then there is no need for a military response on the part of the United States. Since we were looking to define possible future adversary characteristics, we forced each of the targeted nations to be adversarial. However, no guidance was given as to the nature that the adversarial character should assume.

Basically at the beginning of each epoch, each team and its consultant group met in a Decision Day to answer the following six questions:

1. What is the expected threat to your national sovereignty, or what are your territorial or other ambitions, which could generate conflict during the Epoch under consideration?
2. What economic, foreign, and military policies and programs do you choose to pursue for this Epoch?
3. What is the projected size of your national economy for the years of this Epoch?
4. How much of the national economy do you intend to spend on national defense during this Epoch? And, what fraction will go for the creation of the "Access denial Force"?
5. How much of the national defense expenditures will you allocate to each of the following resource allocation categories:
    - A. Current Operations
    - B. Combat System Procurement
    - C. Intelligence (including procurement of intelligence systems)
    - D. Counter-Intelligence and Deception
    - E. Research & Development
        - i. Basic Research
        - ii. Specific Capability Development (e.g., high energy lasers)
        - iii. Combat System Development/Improvement to provide a quantified change in:
            - a. Area Coverage of the Combat System (Detection, Engagement, Control, Command)
            - b. Fire Power (number of targets engageable at a time)
            - c. Responsiveness (time delay)
            - d. Countermeasure Susceptibility Reduction
            - e. Availability of Combat Systems (e.g., logistics, basing structure, etc.)
6. What are the forces anticipated for the end of the Epoch in light of the decisions taken by the Decision Day members? And, what are their projected combat capabilities characterized in terms of the five categories listed in Question 5.E.iii?

Each Decision Day was preceded by several weeks of intense research to generate possible answers to each question. Answers were obtained after significant give and take between the political, economic, technological, and military representatives on the teams.

Given its country's strategy and budget, the student team was free to develop forces and equipment consistent with that strategy and that budget. Resources were allocated among research & development (R&D), manpower, procurement, operations, intelligence acquisition, and counter-intelligence. All aspects of the military (land, sea, air, and space) were considered in the allocations. Specific R&D programs and specific equipment acquisitions were identified. Equipment acquisitions could only be made from those items that had been allocated full R&D funds in prior epochs, or which were available on the international arms market. It was assumed that major arms suppliers (such as France, Sweden, and Russia, to name a few) would not reduce their levels of foreign sales and would not stop developing state-of-the-art weapon systems. The systems engineering faculty validated budget estimates as to R&D cost, and unit equipment costs for every hardware type based on their extensive experience (typically 20 or more years each in the defense industry). The input to the first epoch was the best available intelligence on current budgets, force structures, and defense R&D investments. The consultant groups used the outputs of the first epoch to define the inputs to the second epoch, and the outputs of the second epoch to define the inputs to the third epoch. In this manner, our knowledge of that country in 1999 was projected in a budget- and politics-constrained fashion out to the 2020 time frame. **This approach does not generate a probable future, but does define a plausible, realistic, and achievable one.** The results of this analysis are politically sensitive, producing enlightened forecasts of what potential adversaries might do. To avoid condemning nations for actions they have not yet taken (and hopefully will never take) we will not identify the specific countries studied or their specific responses.

The output of this study (as of early 1999 – the project is still ongoing) was a set of politically and economically constrained force structures as fielded in 2020 for three potential adversaries. The teams representing these adversaries firmly believed that their resulting force structures constituted viable access denial systems that could prevent U. S. power projection. Documentation consisted mainly of a set of videos that recorded the final flag-level debriefings of each of the teams. The results were both fascinating and frightening. Because the force structures were budget-constrained, many potential vulnerabilities were identified and considered whose exploitation could not be afforded because other identified vulnerabilities were selected for exploitation. That one "adversary" decided not to exploit those vulnerabilities does not mean another adversary cannot choose differently. Had the student/faculty composition of a country team been altered, it is likely that the team would have selected a somewhat different set of vulnerabilities. In an attempt to capture more of the work of this program and possibly make a larger positive impact on the military leadership, the author performed this independent analysis of the access denial problem. As the faculty leader of two different teams in successive years, the author had first-hand visibility into many of the debates that led to the final results. Many of the vulnerabilities discussed below were first suggested by the students. Others suggested themselves during more detailed analyses of the earlier suggestions.

CHAPTER 2. VULNERABILITIES & RESPONSES

History has shown that no armed force is absolutely invincible. Changing circumstances require changes in doctrine and equipment that often do not occur in a timely fashion. Despite an awesome collection of military capabilities, the armed forces of the United States are vulnerable to a number of threats. These forces will become even more vulnerable with the passage of time unless significant changes in defense priorities and defense budgets occur in the near future. Many of the vulnerabilities can be exploited by a competitor in the design and implementation of his access denial system. In the following we will summarize our understanding of those vulnerabilities as they apply to the access denial problem. We also summarize those specific actions a large regional competitor or near peer competitor might take to exploit those vulnerabilities and deploy a viable access denial system. One purpose of this paper is to make clear the magnitude of the potential threats faced by our military in this supposed low-threat, post-Cold War environment. A second purpose is to provide a catalog of possible competitor responses to cue intelligence professionals and other military observers to actions that are indicative of a country's attempting to develop the access denial capability that will make them impervious to U. S. influence by military means.

That our military is developing significant potential vulnerabilities has been recognized before. The theme of *Joint Vision 2010* [4], [5] is the creation of a dominant military force, equipped with offensive weapons capable of inflicting unacceptable damage to an adversary and defensive systems capable of preventing unacceptable damage to our own forces, regardless of the task or the adversary. In a 1995 Summer Study [6], the Defense Science Board (DSB) outlined a number of capabilities that an adversary could develop that could be used in asymmetric warfare to counter, negate, or even overwhelm supposed U. S. strengths. These capabilities are listed in Table 2-1. Although the vulnerabilities described in this work were uncovered independently of the DSB study, and address a specific concern in detail rather than a broad concern in general, the correspondence between the DSB list and the author's list (Table 2-2 in the following section) is both striking and significant.

Table 2-1. DSB list of capabilities that 21st century adversaries may pursue to counter U. S. strengths. [6]

Offensive Information Warfare
Weapons of Mass Destruction (WMD)
Reconnaissance, Surveillance, & Target Acquisition (RSTA)
Precision Strike
Counter-RSTA
Camouflage, Concealment, & Deception
Large Numbers of Inexpensive Missiles
Sophisticated, Very Low Observable Cruise Missiles
Land and Sea Mines
Diesel Submarines and Advanced Torpedoes
Underground Facilities

The hypothetical near peer competitor exploiting U. S. vulnerabilities will be referred to as “NPC” in the remainder of this document. The term “near” peer competitor is possibly misleading. A country does not have to be nearly equal to the United States in every aspect. It must only possess an economy robust enough to acquire or develop military forces capable of successfully implementing an access denial system. At least two dozen countries have economies strong enough and military forces large enough to qualify for developing significant access denial capabilities. Several possess the potential to become true peer competitors (and world superpowers) by the middle of the 21st century. One or two of these could become peer competitors within 25 years. The more nearly a peer competitor is a potential adversary, the more vulnerabilities that country will likely attempt to exploit in implementing its access denial strategy. We will use the term “near peer competitor” to refer to any country with the potential to implement any effective form of access denial. By definition, the military of any such country will be able to prevent the United States from exercising its power projection capabilities and influencing regional politics at will. Any such military deserves significant respect.

Fortunately, most of the countries with vigorous (or potentially vigorous) economies are currently friends and allies of the United States and will be unlikely to attempt access denial system development to counter U. S. influence. Unfortunately, at least half a dozen are less friendly and could pose serious threats by the 2020 time frame. More than one of these is almost certain to try to develop an access denial capability. Any country willing to spend on defense over the next 20 years, that quantity of economic resources comparable to what the United States currently spends, would have a formidable military in 2020. This is even more true if that country is willing to abandon any legacy systems it possesses, suffer a period of somewhat reduced military capability, and concentrate on developing and procuring only the best systems most suited to its long-term military objectives. This last approach is something the United States has not been willing to do and it reduces our ability to rapidly restructure our military forces in the face of changing requirements.

It should be noted that it may not take a near peer competitor to develop a viable access denial system. A competitor may possess an access denial capability, yet lack the ability to defeat the United States in a prolonged, high intensity conflict, or even in a single large massed engagement. If a single amphibious task force (carrier battle group plus amphibious ready group) can be successfully prevented from entering a denial zone with limited or remote friendly bases, the U. S. ability to project power will be delayed for a period of many weeks. Additional carriers, amphibs, and pre-positioning ships will be required to transit to a remote rendezvous area, and mass for what might become an opposed amphibious invasion. This delay might provide enough time for the competitor to present the United States Government with a *fait accompli*, to which we are inadequately prepared to respond. In Kuwait, air strikes from an aircraft carrier and the reinforcing of indigenous forces by landing a battalion of Marines might (this is a point of debate) have stopped the invasion, had they been accomplished during the early hours of Iraq’s invasion. Having failed to do this, we required six months to amass an invasion force capable of ousting the entrenched Iraqi forces. Even if a *fait accompli* is impractical, the adversary may be able to inflict enough damage on the initial U. S. forces to cause the U. S. Government to reevaluate whether the benefit of continued conflict is worth the price. All too often, the U. S. projects its power in situations where vital national interests are not at stake. In such instances, an adversary that gives the U. S. a “bloody nose”, such as Somalia [7] or Lebanon [8], can force a U. S. withdrawal.

As a result, we cannot equate economic or political size of a country to whether or not it will possess an access denial capability. Any country (even a small one or a substantial transnational group) can attempt to establish one. Size or economic power will affect only the type and number of vulnerabilities that the adversary can attempt to exploit and the rate at which that exploitation can be implemented.

In each of the following sections we examine a specific area of vulnerability. Each section has the format of a paragraph(s) describing the nature of the vulnerability followed by a paragraph(s) cataloging specific responses that the NPC could and should take to exploit that area of vulnerability. Many of the suggested vulnerabilities are related. In some cases, U. S. attempts to reduce vulnerability in one area have produced one or more additional vulnerabilities. Because the characteristics of these additional vulnerabilities differ significantly from the original vulnerability, we have listed them separately. In a few instances, the vulnerability may not yet be significant, but will likely become significant given the trends currently being pursued by our government. The vulnerabilities described below are loosely grouped by similarity. The order of presentation does not convey any indication of priority or criticality.

Some individuals may take exception to some of the vulnerabilities listed below. They may not believe all of the author’s contentions of how easy it is to defeat one or another of the capabilities of existing systems. Although the author has been directly involved in the development of many kinds of system (or their countermeasures) described here, he will admit that he and the analyses he has drawn upon may not be 100% correct in every instance. However, if only a few of the vulnerabilities described here are as serious as stated, then U. S. forces will face a severe problem in the future. The author also reminds the critical reader that as late as 1996 [9], proponents of GPS guidance were vociferously claiming that such systems could not be effectively jammed. A short time later, critics of U. S. reliance on GPS guidance demonstrated that jamming was relatively easy (with systems reputedly built from approximately five hundred dollars of Radio Shack parts) [10]. The history of electronic combat clearly demonstrates that viable countermeasures can be rapidly developed for any system, no matter how well it is designed [11].

Other individuals may contend that one or more items the author has listed as vulnerabilities are in fact among our greatest strengths. That was almost certainly true in the past. It may even be true at the present time, but the author believes that the United States has become or is in the process of becoming over-dependent on these “strengths”. Over-dependence on an asset turns it from a strength into a liability when the enemy discovers a way to exploit that over-dependence. As evidenced by the ever-escalating spiral of measure and countermeasure in radar and electronic warfare [11], such exploitation is seldom long in coming. It is also true that a factor can be both a strength and a weakness. Our freedom of speech and freedom of the press are major pillars of democratic society. Without them we might not have survived as a free nation. However, none can deny that the press has occasionally published information that is militarily sensitive if not actually damaging. During the Cold War it was often reported that the largest single customer of the Government Printing Office was the Soviet Embassy. If true (and there is no reason not to believe it), it is also clear that the Soviets were not buying every document published out of a benevolent attempt to subsidize an American bureaucratic institution.

Not every weakness will have an obvious remedy. For example, it may not be in the nation's best interests to decrease our societal transparency. Nevertheless, we should be aware that adversaries may take advantage of that transparency and we should try to minimize that potential. We should also make every attempt to increase the transparency of those societies that pose potential future threats. This includes a significant increase in investment in human intelligence (humint) resources.

Some of the proposed threat responses may also seem unreasonable or even to verge on science fiction. To this criticism the author has two comments. First, much science fiction is fiction based on science and any projection of the future is fiction by definition. Verne's [12] nuclear submarine, Wells' [13] atomic bombs, Heinlein's [14] manned space flights to the moon, and Clarke's [15] "intelligent" computers were science fiction when they were written; yet within 50 years each became science fact. As one futurist [16] has observed, "Just because a prediction of future society sounds like science fiction, doesn't make it true. However, if it doesn't sound like science fiction, it will certainly be false."

Second, significant thought by multiple individuals and organizations has been given to every one of the responses proposed in this report. References to published studies and unpublished studies are provided where available. Unfortunately, not all of the analyses of which the author is aware have been adequately documented – in some cases the results have been transmitted "word of mouth" and no hard evidence is known to exist. In these instances, the concept has been reevaluated independently by the author to satisfy himself of the concept's validity before inclusion here. It should be noted that none of the proposed responses violate the laws of physics. With few exceptions (clearly identified in the text) none of the capabilities proposed requires major inventions. They use components that are well within the existing state-of-the-art, although in many cases these components will be combined, juxtaposed, or utilized in novel ways. The primary reasons for the current lack of these systems in the military inventories of our competitors (and our own) include a lack of recognition of need, low priority relative to other technology developments, and inadequate funding, <u>not</u> technical impracticality.

As described above, the following analysis is based on numerous discussions with members of the Naval Postgraduate School Area Denial Project team and its distinguished panel of consultants (which included high-ranking Department of Defense officials, foreign area scholars, former members of Congress, and senior military officers). After several iterations, the author assembled the list of vulnerabilities summarized in Table 2-2. A total of 36 separate areas of vulnerability are identified.

Each of the individual vulnerabilities is discussed below from three perspectives: ***an explanation of how U. S. forces are currently vulnerable or may become vulnerable in the future in the listed area;*** what actions a prospective Near Peer Competitor (NPC) should take (and might actually take) to fully exploit that area of vulnerability; *and what actions the U. S. could or should take to reduce that vulnerability.* The three perspectives will be identifiable by typeface, as shown above. Vulnerabilities will be discussed in the order of their appearance in Table 2-2.

No attempt is made in this paper to prioritize the vulnerabilities or to assign relative probabilities to them. The same is true of actions that the U. S. might take to reduce any vulnerability. No competitor could afford to exploit every vulnerability listed here. The U. S. cannot afford to take every action recommended to reduce the vulnerabilities. Such prioritization is the ultimate goal of this project, however, many more trials with more detailed technical, political, and economic analyses are required. This report is intended to serve as a guide for continued study, as an interim progress report on work accomplished to date, and as a **warning that shortsightedness in planning for future threats may produce results our nation will be unable to live with**.

To help the reader with limited expertise in some of the fields addressed, the author has included a number of technical appendices. Some of these appendices present overviews of broad subjects. Others present detailed technical analyses that would clutter the main body of the text. Some technical training is assumed on the part of the reader, but an advanced degree is not required to understand any of the appendices.

Table 2-2. Vulnerabilities of U. S. forces aiding an enemy's access denial capability.

Attacks Using WMD:	Attack by Nuclear Missiles (ICBMs) Attack by Other Weapons of Mass Destruction
Direct Attacks Against Forces:	Attack by Cruise Missiles Attack by Ballistic Missiles or Superguns Attack by Transatmospheric Aircraft Attack by Naval Mines Attack by Advanced Torpedoes Attack by Advanced Non-nuclear Submarines Attack by Unmanned Air Superiority Vehicles Attack by Infrared Anti-Aircraft Missiles
Counters to Offensive Systems:	Reliance on Stealth Jamming of GPS & GPS-Dependent Systems Jamming of Precision-Guided Weapons
Attacks on C4I Assets:	Attack by Electromagnetic Weapons Attack by High-Energy Lasers Attack by Information Warfare Attack by Antisatellite Weapons Reliance on Long-Range Airborne Surveillance Susceptibility to Strategic Deception Excessive Intelligence-Response Latency
Unconventional Methods of Attack:	Attack by Special Operations Forces Limited Adverse Weather Operations Capability Attack by Nonlethal Weapons
Attacks on Logistics Resources:	Limited Strategic Sea/Air Lift Capability Reliance on Limited Overseas Basing Reliance on Pre-Positioned Equipment Reliance on Underway Replenishment
Attacks on Societal Vulnerabilities:	Civilian Intolerance of Casualties Restrictive Rules of Engagement Civilian Intolerance of Unnecessary Hardships Need for Coalition Support Unequal Societal Transparency Treaty Limitations
Technological Change	Technological Surprise Technological Atrophy Disruptive Technologies

CHAPTER 3. ATTACKS USING WMD

ATTACK BY NUCLEAR MISSILES (ICBMs)

At the present time, the United States and every other country is vulnerable to nuclear weapons in any form. Nuclear explosive devices can be delivered by gravity bombs from aircraft, torpedoes, cruise missiles, or even hidden in cargo or baggage, but especially by ballistic missiles. See Appendix A for a technical discussion of nuclear weapons. ***Intercontinental ballistic missiles (ICBMs) can reach out from protected sites (super-hardened silos or mobile launchers deep in the interior of a country or from ships or submarines in the middle of the ocean) and strike anyplace in the world. Three countries (U. S., Russia, and China) currently possess true ICBM development, production, and launch capabilities. The Ukraine has the facilities to develop and build ICBMs that it markets to the world as satellite launch vehicles. India and North Korea are actively developing ICBMs [17]. Iran is developing a missile with a 5500-km range that is almost an ICBM. The list of ICBM possessors may grow rapidly in the future. Chinese, Russian, or Ukrainian ICBMs may become available for sale to virtually any nation with enough money; their shorter-range missiles are widely exported. Also, any nation that can build satellite launch vehicles can develop ICBMs [18]. In addition to the big three of ICBM fame (U. S., Russia, and China), France, Japan, India, and Israel have repeatedly launched satellites using their own launch vehicles and launch facilities. Italy, Brazil, and North Korea have their own launch facilities and development of launch vehicles is apparently well underway. Spain and Germany are also apparently pursuing development of launch vehicles [17], [19].***

By 2020 it is reasonably certain that the United States will have developed and deployed an effective "National Missile Defense (NMD)" system [20]. See Appendix D for a technical discussion of tactical ballistic missile defense that also explains some critical aspects of strategic ballistic missile defense. ***It is a possibility that this defense will be compliant with the ABM treaty [21] in its current form. If so, NMD will consist of at most 100 interceptors based in Grand Forks ND coupled to a limited number of extremely capable ground-based radars. A space-based sensor component is permitted and will certainly form part of any NMD system. It is anticipated that the space-based component will aid the tracking and discrimination processes, reducing the requirements that the ground-based radars must satisfy. The system will protect most of the U. S. although the Southwest (including San Diego and Los Angeles) and Southeast (including Atlanta and Miami) will not be protected against submarine-launched missiles or missiles that fly great circle routes avoiding crossing the Arctic Circle. Within the covered areas the system will provide high confidence of intercepting all of the warheads that a lesser competitor or rogue state might be capable of acquiring (reasonably assumed to be less than 100). The radar, space-based sensors, and interceptor guidance will be capable of discriminating against many classes of penetration aids (decoys). Precision replica decoys are among the possibilities that would defy discrimination by the sensors being considered.***

However, the NMD system will provide no defense against any warhead that a competitor might possess in excess of 100. As a result it will only provide an extremely limited defense against the nuclear arsenal of a peer (or former peer) competitor such as Russia and it will provide only limited defense to Alaska or Hawaii, Puerto Rico, Midway, Guam, Diego Garcia, or any of our allies (other than Canada). Any system capable of handling more than 100 warheads or fully defending any of these other regions will almost certainly violate the ABM Treaty. Many people are pushing for abrogation of this treaty, and several legal experts have argued that the treaty ceased to be binding when the Soviet Union collapsed [22], [23]. However, to date, both the Executive Branch and the Senate continue to resist this notion and the Russian Federation has denounced any actions in this direction on the part of the United States.

However, if the U. S. is willing to share NMD technology with Russia, Ukraine, Kazakhstan, and Belarus, and/or to provide other substantial economic incentives, there is a reasonable probability that the treaty could be amended to allow limited deployment of additional missiles and/or deployment at other sites. In this case it seems likely that the Grand Forks site would be abandoned in favor of an Alaskan site (the farther north the launch site, the earlier the intercept of any polar trajectory and the larger the impact zone that can be defended). Other sites with additional radar or launcher complexes may also be considered. The current NMD strategy seems to involve a potentially non-treaty-compliant (different site and/or additional radars), evolutionary approach with an initial early 21st century capability of handling a very limited number of "terrorist" missile launches from a rogue state. The "terrorist" threat is assumed to have limited or no penetration aids. As more interceptors are procured, the capability would grow to possess an ultimate capability of handling somewhat fewer than the 100 warheads the ABM treaty allows. At a later date, additional interceptor sites and radar sites could be added to handle more warheads, if it was deemed necessary. It is unclear if the additional radar sites will be capable of the same degree of decoy discrimination as the primary site.

The cost of a treaty-compliant ABM system (as well as the cost of the evolutionary, non-compliant system) is large enough that its deployment would have to be paid for over a number of years. This is one driver favoring the evolutionary approach. It is almost certain that budgetary constraints will limit even a non-compliant system (more than 100 interceptors) to be no larger than 3-4 times the largest compliant system. Such a system would require deployment over several decades. Submarine-launched ballistic missiles (SLBMs) launched from positions just offshore of the Continental United States (CONUS) are not adequately addressed by the current NMD approaches nor are launches from the Southern Hemisphere. As a result several hundred ICBMs and SLBMs should be sufficient to overwhelm any missile defense system the U. S. will be able to deploy in the next few decades. Such a modest strategic force could be afforded by a number of nations, including a few potential adversaries. Thus even with a limited NMD, the U. S. may still face a "Mutual Assured Destruction" situation with several adversary nations. NOTE ADDED PRIOR TO PRINTING: As of the end of December 2001, the Bush administration has notified the Russian government that the United States was withdrawing from the ABM Treaty (as permitted by the Treaty). The Congress has taken no action to prevent withdrawal.

The nuclear arsenal of the United States is aging. As nuclear weapons age, their reliability decreases. In the past we have relied on full-scale testing to maintain safe and reliable nuclear weapons. In 1996 the U. S. signed the Comprehensive Nuclear Test Ban Treaty (CTBT) [24]. Even though the Senate has not yet ratified the treaty, it is may be just a matter of time before this happens. Without the ability to conduct tests, nuclear stockpile stewardship will depend almost entirely on computational modeling and component testing. It remains to be seen if this will be adequate. The U. S. nuclear weapon production program has been closed down for some time, although there is an inventory of "spare parts". When these spares are used up, every weapon withdrawn for reliability degradation or component testing will be one less weapon in the U. S. total inventory. At some point an entire class of weapons might be declared sufficiently unreliable that it would be removed from the inventory. It is unlikely that such weapons would be replaced. It should also be noted that not every potential nuclear power has signed the CTBT. Some of our competitors may not be content to suffer from aging inventories and may keep theirs up to date through continued testing.

The U. S. is also pursuing numerous strategic disarmament initiatives. The more successful these negotiations are, the fewer missiles and warheads the U. S. will have in its strategic deterrent force. Although it is doubtful that the U. S. will ever completely give up its nuclear weapons, in 20-30 years we may have lost several more classes of nuclear weapons and delivery systems. Each reduction in weapons class whether due to age or arms control will reduce the retaliatory options available to military planners. It is possible that we might be left in a position where we could not respond to an opponent's limited use of nuclear weapons (for example, nuclear strikes against our fleets) without resorting to total nuclear war (an option that is just not viable). This is especially important because U. S. naval vessels of every class can be severely damaged by even small nuclear explosives detonated at relatively long ranges. This was proved at the Crossroads Able and Baker nuclear tests in Bikini lagoon in 1946 [25]. A single large thermonuclear explosion centered on the aircraft carrier would damage or destroy most of a carrier battle group.

If it already possesses one, NPC should make sure that it retains a strategic nuclear capability even if the United States develops a National Missile Defense system. Since NPC likely possesses at least a modest nuclear ICBM force, retaining an effective nuclear strike capability in the face of an ABM Treaty-compliant U. S. NMD system will mean making modest increases in the total missile forces. At a minimum NPC should strive to maintain a significant number (perhaps 10 to 20) of missiles in excess of the number of NMD interceptors that the U. S. deploys. To minimize expenditures on additional missiles, NPC may find it desirable to develop advanced penetration aids (decoys) and multiple independently targeted reentry vehicle (MIRV) technology. These improvements in the ICBM force will not present insurmountable difficulties but will require a number of years and considerable investment to accomplish.

Since fixed-site, land-based ICBMs are vulnerable to pre-emptive strikes and the U. S. possesses a variety of means to execute such pre-emptive strikes (ranging from stealth bombers to cruise missiles to ICBMs to special operations forces), NPC may find it desirable to reduce this vulnerability. NPC should investigate developing a mobile ICBM system. NPC should also develop or purchase a ballistic missile nuclear submarine (SSBN) force capable of keeping a substantial number of warheads at sea at all times. As before NPC should attempt to maintain more warheads in both its sea- and land-based missile arms than the United States has ballistic missile interceptors.

If the U. S. abrogates the ABM treaty and espouses a total missile defense posture, NPC should seriously evaluate the possibility that an arms race might be a cost-effective means of maintaining a nuclear deterrence. Purchase of one hundred new, cheap NPC ICBMs for each new deployed, expensive U. S. interceptor complex is a good bargain if the economies of the two countries are roughly equal in size. If the U. S. abrogates the ABM treaty, then NPC should certainly pursue development and deployment of advanced penetration aids. Deployment of such capabilities may render useless many of the lower-cost ABM approaches that the U. S. might be willing to field. NPC should also upgrade its ballistic missile submarine force in a comparable fashion. Operational launch areas for these submarines should be located such that North-Polar trajectories are avoided. In all likelihood, submarine-launched missiles arriving on trajectories from the South, East, or West will be more effective against any U. S. NMD system than will land-based ballistic missiles or submarine-launched missiles arriving from over the Arctic Ocean. Shorter time of flight and depressed trajectories will also improve effectiveness against ballistic missile defenses.

NPC will certainly recognize that any nation that is not capable of delivering a successful nuclear strike against the United States (overwhelming retaliation notwithstanding) will not be considered a peer competitor by the rest of the world. The existence of even a minimal "mutually assured destruction" capability will severely limit the warfighting options of the United States. In Korea, we refrained from bombing critical Chinese targets because we feared nuclear escalation by the Soviet Union. This, at a time when neither side possessed enough nuclear weapons to completely annihilate the other. In Vietnam, the same fear (this time more realistic) prevented our unrestricted bombing and invasion of North Vietnam.

If NPC does not possess ICBMs with nuclear warheads, it should evaluate whether their acquisition is consistent with its long-range plans. Overt proliferation of nuclear weapons and ICBMs will bring strong responses from the United States and all signatories of the Nuclear Non-Proliferation Treaty. The sanctions that result may cripple NPC's economy. If NPC does not have global superpower aspirations, then overt acquisition of nuclear weapons and ICBMs is probably unwise. On the other hand, covert (or at least deniable) acquisition of a limited nuclear capability (even if delivery is limited to covert special operations, such as smuggling into a harbor in the hold of a merchant ship) will benefit any country that anticipates substantial future confrontations with the United States.

NPC should conduct a regular evaluation of U. S. nuclear readiness. If it appears that aging or disarmament has significantly reduced U. S. limited retaliatory capability, then NPC may decide that limited use of nuclear weapons may aid their access denial strategy. If a MIRVed ballistic missile with ten 150 kT warheads was programmed to produce shallow underwater detonations throughout a 100-km diameter impact footprint centered on a carrier battle group, most ships of that battle group would suffer damage that would prevent them from continuing their mission. Such a limited strike that affected only combatant forces would be unlikely to demand massive retaliation on the part of the U. S. If U. S. nuclear retaliation options are sufficiently limited, the U. S. might be forced to simply accept the loss of the battle group. Limited nuclear strikes might also be effective against critical ports or marshalling centers, such as Guam or Diego Garcia. Other "limited" uses of nuclear weapons might include nuclear depth charges for anti-submarine warfare, production of high-altitude electromagnetic pulse, demolition of extremely hardened structures (such as dams), and neutron bomb strikes on isolated land forces. Under no circumstances should NPC use nuclear weapons on the United States proper.

The United States should continue its efforts to curb the proliferation of nuclear weapons and ballistic missile technology. It should also continue to develop a National Missile Defense system. Although NMD will not prevent a near peer competitor from developing a force adequate to establish a mutual assured destruction situation, at a minimum, it will raise the ante with respect to another nation's being able to hold the U. S. hostage to its nuclear weapons. The United States should give careful consideration to implementing any NMD beyond that needed to defend against the minimal threat (terrorist, renegade, or accidental launches). Any capability beyond the minimum may inspire an adversary to engage in a one-missile-for-one-interceptor arms escalation that could favor the adversary from an economic perspective.

The Stockpile Stewardship program should make every effort to validate the trustworthiness of the computational "systems" – Software and Hardware – used to predict the stability and reliability of our nuclear stockpile. This will almost certainly require the completion of the National Ignition Facility (NIF) to permit critical and thoroughly instrumented testing of tiny thermonuclear devices that can be used to validate the software by comparing computational predictions with the results of experiments. Should the NIF suffer from funding cuts or otherwise fail to become operational, then the U. S. should reconsider its stance on the Comprehensive Test Ban Treaty and on continued adherence to a testing moratorium.

ATTACK BY WEAPONS OF MASS DESTRUCTION

Weapons of Mass Destruction (WMD) in this section are intended to mean any form of chemical, biological, or radiological (CBR) weapon. Although nuclear explosives are clearly WMD, they have been addressed separately by the preceding paragraphs. See Appendix A for a detailed technical discussion of all kinds of WMD (nuclear, chemical, biological, and radiological). Many nations possess WMD capability. ***The Federation of American Scientists estimates that there may be 25 countries with chemical weapons programs, 19 countries with biological weapons programs, and 1 with a radiological weapons program, although some of these countries have pledged to destroy any weapons and weapon production facilities that they possess [26]. Some of these countries are openly hostile to the U. S., while others cannot be considered as friendly. If hostilities arise between these countries and the United States, there may be few good reasons for them not to use these weapons against U. S. forces.***

Ships of the U. S. Navy have mixed vulnerability to WMD. Most warships and support ships possess a countermeasure washdown system [27]. In theory, the sea water spray from this system will wash a large fraction of any aerosol contaminants out of the air before reaching the ship's surface. The spray will also wet the surface of the ship and make it less likely for remaining contamination to adhere to the surface. Finally, the runoff will wash away much of the contamination. However, the washdown system is infrequently tested (several times a year) and is both subject to corrosion problems and is a source of corrosion in other systems. It may not function properly when necessary. Even if it does function, it requires a human operator to activate it. If not activated in time (because the agent delivery occurs too quickly for effective response or because a WMD attack is not recognized as such until it is too late), significant surface contamination will result. The spray system typically does not protect the uppermost part of a ship's superstructure and masts. Wind and ship motion can also result in incomplete coverage of portions of the hull and lower superstructure. The uncovered areas will almost certainly become severely contaminated. The washdown system coupled with fire hoses and scrubbing and swabbing will only partially decontaminate the exterior of the ship. Special decontaminating agents (such as DS2 or HTH) and decontaminating equipment are required to thoroughly decontaminate the ship. HTH (calcium hypochlorite) is the only decontaminating agent routinely available on Navy ships, but it is not usually carried in sufficient quantities on surface combatants.

Most of our warships have been provided with limited collective protection capabilities. However, the DDG-51 class is the first ship class designed to have a full collective protection system. This will protect most of the crew for extended periods of time, if the collective protection system is functional and if the WMD agent is not introduced into the enclave (e.g., due to battle damage or by intentional hull penetration by the warhead). Older combatants, carriers, and amphibious ships have been retrofitted with collective protection of selective spaces. The protected spaces usually center on the Combat Information Center (CIC), but often do not include crew berthing and messing spaces. Non-combatants (e.g., logistics ships) usually do not have any collective protection systems, although they do have ventilation systems that can be closed down and hatches that can be secured to create spaces that are resistant (but not completely impervious) to CBR agent penetration. This last form of protection might provide a

crew survival shelter for limited periods of time (CBR contamination will ultimately penetrate these spaces if exposure continues).

Once contaminated, surface combatants may be able to fight buttoned up for extended but limited (one or two days) periods of time; however, aircraft carriers, amphibious ships, and logistics ships cannot conduct their primary operations in a fully buttoned-up condition [28], [29]. If the hangar decks, well decks, or cargo holds are opened for operations prior to complete external decontamination, the interior spaces will also likely become contaminated. If these spaces are open when an attack occurs, severe interior contamination is almost certain. This would necessitate cessation of all operations for days of thorough decontamination or force all operations to be conducted in MOPP 4 (Mission-Oriented Protective Posture 4 – wearing of the full CBR protective clothing ensemble), with its concomitant serious degradation in performance. If a ship were to be contaminated with a biological "Andromeda Strain" agent [30] especially designed for persistence, it is doubtful that it could ever be perfectly decontaminated. Lacking assurances of complete safety, every port facility in the world (including possibly our own) would likely refuse entry for the ship (and possibly its crew) [1] until the ship finally rusted out and sank.

Although ship and crew may survive conventional WMD attacks, we possess very little true defense capability against unconventional weapons such as WMD sea mines, ballistic missiles with WMD warheads, or torpedoes or cruise missiles with combined armor piercing/WMD agent warheads. WMD sea mines can produce low altitude airbursts of agent directly over ships within seconds of when they are triggered. Indeed, during the heyday (early 1950's) of the U. S. biological warfare program, the U. S. Navy developed a submarine-deliverable mine containing a biological agent [31] (almost certainly anthrax). Combined armor piercing/WMD agent warheads are designed to penetrate collective protection enclaves and introduce the WMD agents into the interior of the ship. Ships are also vulnerable to sabotage from WMD devices or agents hidden in fresh food and other stores that are on-loaded during port visits or carried aboard by visitors to the ship. They are even more vulnerable to chemical and biological sabotage by deep cover agents who are part of a ship's crew. Given the multi-cultural character of the United States it is virtually impossible to exclude members of any ethnic heritage from service in the armed forces. It is equally impossible to run full background investigations on every service member to turn up suspected agents.

Other military units that contribute to force projection also have limited vulnerabilities to WMD. If aircraft fly through a contaminated environment, they will become externally contaminated. Systems are available for protection of the aircrew and for efficient decontamination of the aircraft. The necessity for decontamination will of course impose operational and performance inefficiencies. If WMD is deployed on the friendly facilities being used for strategic airlift and/or sealift, the transport airport and ships will become thoroughly contaminated inside and out. Unloading operations can still be undertaken, but continuous MOPP 4 operation will take its toll on efficiency. The necessity to decontaminate the interiors of strategic transport aircraft will dramatically reduce cycle time and could reduce airlift rates by 50% or more [1].

U. S. vulnerability to CBR weapons is enhanced by an asymmetric policy. Since 1978 the official U. S. policy has been:
"The United States will not use nuclear weapons against any non-nuclear weapon state party to the NPT [Non-Proliferation Treaty] or any comparable internationally binding commitment not to acquire nuclear explosive devices, except in the case of an attack on the United States, its territories or armed forces, or its allies by such a state allied to a nuclear weapon state, or associated with a nuclear weapon state in carrying out or sustaining the attack." [32]
That is, if attacked with CBR weapons by an NPT signatory state, the U. S. has pledged not to retaliate with nuclear weapons. If conventional hostilities are already occurring between this state and the U. S., this policy denies the U. S. its most significant mode of retaliation.

NPC should determine its position vis-à-vis first use of chemical, biological, and radiological weapons. If first use is not ruled out, and especially if NPC has decided it cannot have a nuclear weapons capability, it should develop or expand its capabilities to develop, test, and produce selected CBR agents. As there are world sanctions against developing chemical or biological weapons, this program should be carried out covertly. In the case of chemical agents, the agent production facilities can easily be masked as pesticide or pharmaceutical plants. In the case of biological agents, the production facilities can be hidden in any large manufacturing complex, disguised as civilian biotechnology facilities, or built into self-contained mobile units disguised as commercial semi-trailers (and continually driven from one site to another to avoid outside inspection).

NPC should develop equivalents to the "Public Health Service" and the "Center for Disease Control". These entities should participate in worldwide World Health Organization activities. This will provide "legitimate" access to emerging pathogenic organisms and provide cover for maintaining biosafety level 4 facilities [33]. This would greatly facilitate developing biological weapons as well as biological weapon defenses, and if the masquerade is carried beyond the walls of these facilities, it would ultimately significantly improve the health of NPC's citizens and military personnel, just as the CDC has done in the United States. Testing of chemical and biological weapons should be done at remote test sites with a minimum of permanent facilities or in underground facilities. This will make it difficult for the U. S. to monitor and correctly identify the character of the tests.

NPC should develop or expand it capabilities to defend its own forces against WMD use by others. It should develop advanced personal protective equipment, chemical/biological agent detection equipment, and prophylaxis against known chemical and biological agents in the inventories of potential adversaries. It should produce classical WMD munitions and integrate them into its land and air forces. It should also develop a practical antiship WMD capability. This last capability (mines, missiles, and/or torpedoes) should take the form that fits best with NPC's general military capabilities. It should also begin/continue a process of positioning loyal NPC agents throughout American society. Over 20 years it should be easy to infiltrate tens of thousands of agents into American society. At this level there would be few organizations of any type, that did not have at least one NPC agent with access to its inner workings. At the start of any conflict, these agents could cause sabotage with WMD on a grand scale, in addition to gathering critical military, political, economic, and technical intelligence. Such a "fifth column" activity should be initiated for its intelligence and conventional sabotage potential even if use of WMD is renounced.

The United States should continue its efforts to curb the proliferation of weapons of mass destruction. It should strive to include effective enforcement measures into each non-proliferation treaty it negotiates. The United States also needs to improve the defensive equipment available to its military forces. Although many improvements are being actively pursued, some are not being pursued at all and many others have performance objectives that are inadequate to meet potential future threats. Personal protective equipment needs to be capable of protecting individuals for many days without degradation and of being decontaminated, refurbished, and reused without requiring extensive special facilities. Collective protection systems need to have airlocks combined with decontamination capabilities that will permit rapid ingress and egress from contaminated environments. Environmentally safe and non-toxic decontamination agents need to be developed that can be used to rapidly decontaminate sensitive equipment, such as aircraft electronics. Naval vessels need to be designed to be able to conduct their entire range of operations for extended periods of time in heavily contaminated environments. This will involve radical design changes to some ship classes such as amphibious ships, logistics ships, and aircraft carriers to permit vehicles and cargo to be decontaminated and have rapid access to/from collectively protected spaces. Vaccines need to be developed for all significant microbiological agents. Antidotes and safe and effective pre-treatments need to be developed against chemical and toxin agents.

CHAPTER 4. DIRECT ATTACKS AGAINST FORCES

ATTACK BY CRUISE MISSILES

Antiship cruise missiles continue to pose serious threats to U. S. naval forces. As demonstrated by the 4 May 1982 sinking of the HMS Sheffield [34], [35], the 25 May 1982 sinking of the SS Atlantic Conveyor [34], the 6 June 1982 damaging of the HMS Glamorgan [34] (all three during the Falklands War), and the severe 17 May 1987 damaging of the USS Stark during the Iran-Iraq War [36], all by relatively small Exocet cruise missiles, cruise missiles are proven ship-killers. The Exocet carries a warhead containing only 60 kg of high explosives. Most cruise missiles have larger warheads and are even more lethal.

Active cruise missile defense requires early detection and tracking of incoming missiles and high-speed agile interceptors to kill the cruise missiles before they get close enough to the ship for debris (from a destroyed missile) to impact and damage the ship. Unfortunately, the low radar cross sections coupled with multipath (interference due to radar returns reflecting from the sea surface) and refractive ducting make detection of sea skimming missiles difficult at long ranges. Even scheduled improvements to the Aegis fire control system will not provide high certainty detection of very-low altitude missiles in multipath and ducting environments at ranges long enough to guarantee intercepts and avoid damage from postulated advanced threats. Operation in littoral waters will provide close-in launch opportunities to land-based or small-craft based missile launchers. Even the inclusion of the much-needed Cooperative Engagement Capability (CEC) [37] into the Navy's weapons command and control systems will provide minimal advantage if the enemy employs a rollback attack. In such an attack, a first wave targets and sinks or damages the outer ring of picket ships (these gain only limited advantage from CEC in terms of improved detection or warning). A second wave well behind the first takes out the next ring of CEC-equipped ships. The loss of the outer picket ships almost completely eliminates the supposed CEC advantage of ships in this second ring. Third, fourth, and fifth waves successively reduce the rings of defensive capability until the high-value targets are overwhelmed.

Cruise missiles will become faster, more agile (even to the point of violent maneuvering), and more surface-hugging (advanced autopilots will be capable of measuring local sea state and picking the lowest cruise altitudes that provide marginally acceptable wave clobber probabilities). Future cruise missiles will likely employ combined RF and IR seekers for countermeasure resistance. <u>See Appendix G for a detailed description of missile guidance techniques</u>. ***The missiles may even carry their own self-protection jamming systems just like manned aircraft. On a large, long-range cruise missile the penalties associated with carrying jammers or multiple expendable aerodynamic decoys (possibly including active emitters as well as retroreflectors for passive cross section simulation) are not likely to be insurmountable. The generation-after-next of cruise missile seekers will almost certainly be capable of determining and hitting the most vulnerable point(s) on any class of target. If the U. S. fails to develop directed energy weapons, then U. S. surface forces will be readily vulnerable to***

"magazine" saturation, that is, attack by more threat missiles than the U. S. forces have interceptor missiles with which to counter them. This is one of the threats highlighted by the Defense Science Board. It was also a tactic independently adopted by every red team in NPS' Area Denial study. Even a country with a relatively modest economy could afford to procure tens of thousands of low-cost antiship missiles. If country X has 20,000 missiles in its inventory, it can easily afford to fire 1000 missiles at a single carrier battle group. It is noteworthy that recent Net Assessment wargames have begun to include similar large missile inventories in the adversary's order of battle [38].

In recent years, surface ships have relied on layered active defenses involving aircraft, long-range missiles, short-range missiles, guns, electronic jammers, and decoys [39]. However, a ship or battle group can carry only a finite number of missile kills in its inventory. One thousand missiles exceeds the most optimistic number of available kills that even a battle group would possess. Appendix B presents a detailed analysis of the active defense of a battle group. ***The bottom line is that after every defensive weapon in the battle group is used up, many dozens of attacking missiles still remain to complete the destruction. Assuming a standard defensive weapon mix available today, a quantity exceeding 140 missiles (out of a salvo of 1000) survives to hit the 7 major combatants assumed to make up the battle group. This averages to 20 missile hits per ship. Even with an improved weapon mix, 40 missiles survive to hit the battle group (giving 5-6 hits per ship).***

No matter how many missiles an adversary possesses or how lethal those missiles may be, those missiles will not pose a threat if they cannot be allocated against targets of importance. Targeting ships at sea has always been a difficult proposition. The ocean is large and ships are small. At long ranges, it is difficult to detect a battle group let alone a single ship. Once detected, the ability of a ship to move makes it hard to hit. Given perfect knowledge of initial position and velocity, the missileer can only fire at a predicted position. At long ranges, missile times of flight become long. A Mach 0.9 missile requires 1000 seconds to reach 300 km range. During this same period a 30-knot warship can move more than 15 km. The uncertainty region in target position can be as large as 15-20 km in radius. If there is a time delay between detection and launch, the uncertainty region can grow larger proportional to the delay. If there is an uncertainty in the original position (due to sensor accuracy), this will add to the size of the ultimate uncertainty region. To complement the adversary's missiles, he must have a targeting system that has high detection probability, good localization accuracy, and short sensor-to-shooter communication times. This is true whether the adversary is using subsonic cruise missiles, supersonic cruise missiles, ballistic missiles, torpedoes, or "superguns" [40]-[42]. Traditionally, the targeting system has been harder to implement than the missile system.

NPC should continue to improve its position with respect to cruise missiles. It should develop or buy faster (Mach 3-5), more agile (15-30 g), and longer-range (300-1000 nmi) missiles. It should equip those missiles with combined RF/IR imaging seekers and more lethal warheads. It should incorporate self-protection jammers and/or expendable aerodynamic decoys into the missile payloads. It should procure these missiles in enormous quantities. Since this may arguably be the single most important component of an access denial system, it is not unreasonable that a significant portion of the defense budget should be devoted to cruise missile acquisition. NPC should be willing to expend enough missiles in each attack to guarantee overwhelming the U. S. defenses. That may turn out to be a significant fraction (5-10%) of the total missile assets unless NPC can afford to procure enough missiles to make the fraction smaller.

NPC should develop launch platforms, targeting sensor systems, and command & control networks capable of allowing NPC to strike at U. S. naval forces at extremely long ranges from NPC territory. It should procure adequate launch platforms to conduct the massive strikes described in the preceding paragraph. It should develop multiple systems capable of providing the needed targeting data. NPC should consider space-based imaging, space-based electronic support measures, space-based radar, underwater acoustic sensor arrays, underwater arrays of sensitive magnetometers, and/or airborne radar technologies for the targeting role. A high degree of integration between different sensor systems and between sensor systems and weapon systems is desirable. If NPC can kill enough U. S. surface combatants before those combatants come into Tomahawk missile range of critical targets, the traditional rollback approach of the carrier battle group can be negated. Failure of the rollback approach (i.e., using cruise missiles to defeat the air defense and C^2I systems, followed by long-range aircraft to achieve air superiority, followed by strike aircraft and amphibious forces to project power ashore) will inevitably lead to new strategies. Some of the proposed alternatives are based on increased utilization of Air Force assets and Army airborne assault forces. Should the alternatives come to be accepted, it might result in the eventual disappearance (for lack of a mission) of any substantial U. S. overseas naval presence.

The United States needs to develop new defensive systems against cruise missiles. Such systems must provide vastly more kills per ship than the best existing systems. High capacity launchers of small missiles (such as the 21-missile RAM launcher) are one option although longer range, more capable missiles are desirable to defeat more capable future threats. Directed energy weapons (DEW) have the potential for even more kills per weapon than multiple missile launchers. Only limited development is needed to field improved microwave and infrared active jammers against infrared missiles. The United States should expedite the advanced development and weaponization of free-electron lasers as anti-missile systems. Renewed effort should be expended to determine if alternative directed energy devices have the potential to be used as shipboard weapons. Current fire control systems are not capable of supporting these new weapons. Improved sensors for longer-range, higher resolution detection, tracking, and handover (to missile seekers or DEW aiming sensors). Even current fire control systems should be investigated to determine their susceptibility to missile jamming or expendable decoys. If these susceptibilities are severe, then development of counter-countermeasures is warranted.

Unless fantastic improvements are made in both quantities and kill probabilities of anti-missile systems, naval vessels subjected to massive cruise missile attacks will be hit by one or more missiles. Naval ships should be designed to survive such missile hits. This may involve incorporation of additional armor, ballistic protection of interior compartments, relocation of critical systems (such as the bridge) to more survivable interior spaces, and widespread use of automatic flash & fire suppression *systems. Given the increased likelihood of damage, the U. S. should pay increased attention to damage control techniques and damage repair (recovery) equipment and techniques.*

ATTACK BY BALLISTIC MISSILES OR SUPERGUNS

Theater ballistic missiles include any self-propelled weapon following a ballistic trajectory that does not both carry a nuclear warhead and travel intercontinental distances. The U. S. is actively pursuing defenses against theater ballistic missiles. The first generation (Patriot PAC-3 and Standard Missile Block IVA) of theater missile defense (TMD) systems will provide limited area defense (including point defense) against short-range (<500 km range) missiles. See Appendix C for a technical discussion on missile nomenclature, Appendix D for a technical discussion of ballistic missile defense, and Appendix G for a technical discussion of missile guidance techniques. ***Intercepts will be made within the atmosphere, as the interceptors will utilize aerodynamic controls. The next generation (THAAD and Navy Theater Wide) of TMD systems [43] will be located forward and designed to protect rear areas from attack by medium-range (500-1000 km range) and intermediate-range missiles (1000-3500 km range). The "kinetic kill vehicles" of the next generation systems will make exoatmospheric (altitudes nominally above 100 km) intercepts using divert motors for aiming control. These new TMD systems will have the capability to defend themselves against short-range and medium-range missiles, but possibly not against intermediate-range and long-range (3500-5500 km) missiles.***

The longer the range of a ballistic missile, the faster it travels. Faster incoming missiles must be detected at longer ranges in order for an intercept to be achieved at a desired "keep-out" distance. All other factors being equal, longer detection ranges means larger radars (75% larger linear antenna dimension to detect a 1500-km range missile vs. a 500-km range missile). See Appendix E for a technical discussion of radar systems performance. ***Against intermediate-range and longer range missiles, the radar needed to detect reentry vehicles, to discriminate them from decoys and debris, and to track the reentry vehicles at ranges sufficiently long to permit a self-defense intercept may well violate the ABM Treaty.*** See Appendix L for a thorough discussion of the provisions of relevant arms control treaties. ***If the U.S. deploys a TMD system, then a threat desiring to have a ballistic missile capability can make three responses: build more missiles than the U. S. can build interceptors, build very fast, long range missiles that the TMD system cannot intercept, or deploy penetration aids similar to those used with ICBMs. The best strategy may be a mixture of all three. Older less capable missiles fitted with penetration aids can be used in an initial salvo to attrit the defensive missiles prior to an attack by the more capable missiles (also carrying penetration aids to insure their survival to strike the targets).***

The ABM Treaty also limits the performance of missile defense components such as radars and interceptors that are not specifically ABM components. Under the ABM treaty, only two radar units per country can have power-aperture products greater than 3,000,000 W-m^2. All other radars must have smaller products. The power-aperture product is the product of the mean power emitted by the radar in Watts and the area of the radar antenna in square meters. 3,000,000 W-m^2 corresponds to a 10 meter diameter radar radiating an average power of slightly less than 40 kilowatts. A typical large shipboard air search radar has a roughly 4 to 6 meter diameter antenna with an average radiated power of roughly 2 kilowatts. Such radars lack the power-aperture product to track longer-range missiles at ranges of interest. It will be

difficult to integrate larger missile defense radars into the limited size of a ship's superstructure.

The current generation of TMD missiles will have limited speed and agility and will have difficulty performing an endoatmospheric intercept against incoming reentry vehicles that are much faster than those of short-range missiles. The next generation will lack an endoatmospheric intercept capability (due to lack of seekers capable of operating within the atmosphere at higher interceptor speeds and the desire to intercept the warheads earlier in their flight). Given limited radar detection/tracking ranges, the interceptors will need even higher speed to achieve exoatmospheric intercepts in a self-defense mode. Thus, it is doubtful that the next generation of TMD missiles can be made to be capable of self-defense against intermediate range ballistic missiles unless a separate sensor (probably airborne or space-based), that can generate the necessary tracking data earlier than the radar, can be added to the system. The U. S. will have space-based sensors associated with its National Missile Defense capability. It is possible, but not assured, that the space-based assets could provide the needed tracking. They might also be capable of providing additional discrimination. It is doubtful that these sensors will be capable of discriminating against all practical decoy systems.

Against long-range missiles (3500-5500 km range) or "intercontinental" ballistic missiles (range > 5500 km) any component of any viable defense system (self- or rear-area) will of necessity violate the ABM Treaty (unless it is never tested against its intended targets – an unlikely occurrence for a deployed system). See Appendix L. ***It will likely be several years at least before enough Senate support is mustered for abrogation of the ABM Treaty to be seriously considered or for approval to be granted to give the TMD technology to Russia in exchange for a negotiated amendment to the treaty. It would be difficult to upgrade any of the radars in the fleet to provide the extended range and decoy discrimination capability needed for self-defense against intermediate-range or longer ballistic missiles or against even medium-range missiles carrying penetration aids. It would be cheaper (if not essential) to develop a new class of ships and the first of such a class would not likely be deployed before 2030.***

Another problem in defending against ballistic missiles is the small number of shots available to the defender. Even if a dedicated missile defense ship were deployed with each battle group, it will have a limited number of interceptor missiles. Given reasonable missile reliabilities and hit probabilities, the number of missiles that can be destroyed is much less (realistically not greater than 80% and possibly less than 50%) of the number of interceptors available. Magazine saturation attacks similar to those described in the section on cruise missiles are a viable option. An adversary can afford to spend $100 million on ballistic missiles if it means almost certain sinking of a $1 billion dollar warship (and destruction of a significant fraction of our power projection capability). It is also likely that an interceptor missile will cost more than the ballistic missile it is designed to counter. Cost to the adversary may be reduced if he uses older less capable and less costly missiles early in such magazine saturation attacks. Every missile is a threat if it is not defended against. An interceptor for each ballistic missile arms race is not one the defender usually wins. The cost disadvantage is one of the reasons (but by no means the only one) that the United States negotiated the ABM treaty in the

first place. Even with economic disparities, the U.S.S.R. could afford to build ICBMs faster than the U.S. could afford to build ABM missiles

.

The self-defense threat to U. S. forces at sea is potentially very real and significant. Even if the possibility of warheads carrying nuclear explosives or chemical, biological, or radiological agents can be discounted, the threat from conventional warheads is substantial. The Pershing II missiles deployed by the United States in the 1980's could carry conventional warheads as large as 500 kg (although only nuclear warheads were ever deployed – Pershing II was a strategic disarmament chess piece from the beginning) [44]. Although not originally intended to do so, a Pershing II had the guidance accuracy to hit a ship at 1500 km range (if a ship's signature had been programmed into the radar terminal guidance instead of the traditional airfield or command bunker targets). Given a nominal 15-minute flight time, the limited terminal maneuver envelope might have prevented the Pershing II reentry vehicle from attacking high-speed ships that performed an evasive maneuver shortly after launch (and thereby moving 10-15 km away from a predicted aimpoint). However, that limitation could have been eased by relatively straightforward design changes, had an antiship role been envisioned, or it could have been countered (at the expense of wasted missiles) by firing several missiles in a salvo at slightly different predicted aimpoints to compensate for the maneuvers.

The number of limited-footprint missiles wasted in attacking a battle group would actually be relatively small since any maneuver of a ship near the center of the group would likely bring it under the footprint of a missile intended for another nearby ship of the group. Twenty Pershing IIs would probably be enough to destroy the six to ten surface ships in a typical U. S. carrier battle group. There are no technological hurdles preventing other countries from developing terminally guided antiship ballistic missile capabilities superior to the Pershing II's. Such missiles would be relatively immune to attack by existing and planned Theater Air Defense systems. In fact, land-based TMD systems would make excellent targets for a Pershing II-like missile. Once the TMD systems have been eliminated, then any ballistic missile could be employed to maximum effect. The ability of an adversary to target and sink naval vessels thousands of kilometers out at sea from deep inland launch sites that are virtually untargetable would force current U. S. naval strategy to be drastically revised. It should be noted that numerous sources indicate that both India and China are developing terminal guidance systems similar to Pershing II's for their intermediate-range ballistic missiles [45-48].

Ballistic missiles might also play a significant role in the air war. A ballistic missile can carry conceivably carry several dozen lock-on-after-launch air-to-air missiles as submunitions and dispense them just as the reentry vehicle enters the stratosphere. Each submunition is individually capable of targeting and downing a different aircraft. Descending from above (conceivably without useful warning) on a large flight of aircraft (such as a bombing raid) or over an aircraft carrier conducting launch or recovery operations associated with a large strike, the submunitions from a single ballistic missile could annihilate much of an entire air wing. It is important to note that the top-down view is typically the direction considered of least importance in stealth design. Thus, even stealth aircraft would be at risk from ballistic missile-delivered weapons.

Missiles are one means of delivering ballistic projectiles at long ranges. Guns, or more properly "superguns" [40]-[42] are another. These large-caliber guns are capable of firing multi-tonne projectiles over distances of hundreds of kilometers, if not farther. In the 1960's the High Altitude Research Programme (HARP) used a modified 16-inch gun to fire Martlet missiles to altitudes as high as 180 km [41]. Before the Gulf War Iraq was constructing a supergun for use against hostile nations in Southwest Asia (most likely Iran and Israel). [42] This supergun was intended to have a 1000 mm diameter and be 172 meters long. A 350 mm diameter, 45 meter long prototype had been built earlier. China has reportedly developed a 406 mm diameter gun mounted on a modified M-11 ballistic missile carrier. Firing terminally-guided rockets with over 360 km range, this gun is capable of delivering high explosive, incendiary, ground-penetrating, cluster munition, or anti-armor submunition warheads anywhere in Taiwan from the Chinese mainland. Effective warhead radius (cluster?) is supposedly 450 meters. Guidance is said to include GPS, television, infrared, and laser sensors. [256], [257] In addition, the United States is studying superguns as possible low-cost satellite launch systems [40].

Superguns with ranges in excess of 100 km will be large (tens of meters to perhaps as long as a kilometer). Smaller devices may be transportable on large vehicles similar to those used for transporting and launching mobile ICBMs. Such guns will be aimable to cover any target within their range. Larger guns will be fixed installations. However, this does not mean that the guns are not "aimable". Divert thrusters on the projectile, fired shortly after clearing the gun tube, should be capable of altering the final trajectory by a few degrees or more. Asymmetric injection of propellant at the gun muzzle will induce a tipoff which should accomplish similar angular deflection of the trajectory. At a nominal range of 1000 km, +/- 5 degrees corresponds to a cross range deviation of +/- 85 km. Longer ranges will yield larger possible deflections. This is enough to cover the important regions of many small countries such as Israel or Taiwan, or to completely cover a classical choke point such as the Straits of Hormuz, the Suez or Panama Canals, or the English Channel. Furthermore, a single propellant facility should be able to service a number of gun tubes. A half-dozen gun tubes (each being aimed 10 degrees different than the trajectory of its neighbors), yet sharing a single propulsion system, would provide enormous coverage at a small increase in price over a gun with a single barrel. The gun tubes are cheap compared to the costs of putting the propulsion and support structures in place. The projectiles fired from superguns can be terminally guided to permit any target in the gun's footprint to be attacked and destroyed.

Superguns will have limitations on their rate of fire. Large projectiles cannot be loaded into such a gun as quickly as bullets can be loaded into a machine gun. The intense heat deposited in the gun barrel will need to be removed to prevent the barrel from warping. However, taking these factors into account, a rate of fire of one round per minute is not unreasonable. This is one or two orders of magnitude faster than a ballistic missile transporter-erector-launcher (TEL) is capable of being reloaded and refired. Superguns will have a finite barrel life. The higher the projectile velocity that is developed, the shorter the barrel life. If a supergun is used for orbital insertion, the barrel life may be as short as one shot. For a 1000 km range, barrel life may be as short as a few dozen shots. All current artillery guns must replace the barrel after a specified number of shots (of the order of several hundred to several thousand rounds). A sensible design would provide for rapid replacement of the lining of the

barrel without replacing the entire barrel. Note that even a ballistic missile launcher must be completely refurbished after a limited number of firings, so short barrel life is not an overwhelming disadvantage.

Given the ability of superguns to fire enormous projectiles at ranges comparable to ballistic missiles, it should be obvious that everything said in the preceding paragraphs about ballistic missiles holds for supergun weapons as well. Indeed, the gun projectiles might be directly adapted from the reentry vehicles used on existing ballistic missiles.

NPC should develop and deploy intermediate-to-long-range ballistic missiles (3000-4000 km range) capable of delivering 1000 kg conventional warheads against moving ships anywhere within a 50 km diameter error basket by employing terminal seekers with better than 10 m guidance accuracy. The launchers and support equipment should be mobile, to reduce the possibility of counterstrikes. A low-latency time (< 5 minutes), accurate (< 5 km position error) ocean surveillance and tracking system should be developed to provide the detailed targeting information needed to coordinate an attack. The post-boost vehicles should be capable of dispensing penetration aids to reduce any possibility of shipboard radar discrimination, tracking, and intercept of the actual reentry vehicles. Such missile would not only facilitate access denial, but also attack of critical ground targets, including those defended by any missile defense system short of an ABM-treaty violating design.

NPC should consider using any of its older medium-range ballistic missiles as "armed decoys" to facilitate attacks by more capable missiles. These missiles should be retrofitted with penetration aids. If fired first, the older missiles must be countered by the U. S. TMD system as they are still lethal threats. If enough of the cheaper shorter-range missiles are available they may completely deplete the magazines of the U. S. TMD system, allowing a handful of truly capable (and more expensive) weapons to be assured of hitting the targets of interest.

NPC should also investigate developing air-target submunition payloads for ballistic missiles. These submunitions can make use of their reentry velocity for maneuver. This negates a need for propulsion. Because of the high velocities at reentry, infrared seekers may be precluded due to excessive window heating. The air-target submunition will therefore probably employ active radar terminal guidance. This should be effective even against current stealth aircraft designs as the submunitions will target and attack from near the zenith. The zenith is one angle at which stealth designers do not yet expect to find threat radars, thus cross section is not minimized from this direction. The submunitions would probably carry proximity-fuzed fragmentation warheads to avoid the need for hit-to-kill. This would also increase kill probability against highly maneuverable aircraft such as unmanned air superiority vehicles. A viable anti-air ballistic missile capability would allow NPC to attack U. S. carrier aviation assets at the most inopportune times (for the aviators), such as launch or recovery of a major strike, at almost any range, with very limited warning, and almost negligible risk to NPC assets.

NPC may also wish to investigate the development of superguns. Although superguns typically require fixed sites and have limited angular coverage, they have the distinct advantage of relative high rates of fire (much higher than reloadable ballistic missile launchers). It should pose little problem to design a supergun capable of firing several 1000-kg terminally-guided projectiles every minute for many minutes. Built into a tunnel, a single supergun might be capable of blanketing with fire and effectively closing down one or more strategic choke points (such as the Straits of Gibraltar, Hormuz, Malacca, or Tsushima) and be relative secure from counterattack.

The United States needs to recognize the probable total scope of the future ballistic missile threat. Defending against inaccurate battlefield missiles, such as Scuds, is useful. However, by 2020, the real killers will likely be missiles with capabilities more like a Pershing II, rather than like a V-2. We need to recognize that mobile targets (including ships at sea) will be able to be attacked by intelligent, guided ballistic missiles with conventional warheads. Any ballistic missile defense system should have a realistic self-defense capability against the longest-range (>3000 km) terminally guided ballistic missiles. Otherwise, the missile defense systems are likely to be among the first targets. Self-defense will probably require interceptors with higher velocities and kill vehicles with excellent decoy discrimination as well as enhanced divert capabilities. The United States should consider abrogation or renegotiation of the Anti-Ballistic Missile Treaty to permit deployment of ABM-quality missile defenses at overseas locations and on selected naval vessels. To facilitate the latter, research into improved long-range radars or other detection and tracking sensors such as integrated passive infrared and laser radar systems should be encouraged. Laser radars have real possibilities in discriminating against even precision replicas. Incorporation of these capabilities into space-based sensors should be actively pursued. The development of active seekers using ladar techniques might also solve the discrimination problem without changing the character of the space-based sensors.

ATTACK BY TRANSATMOSPHERIC AIRCRAFT

The United States is actively pursuing the development of transatmospheric aircraft (TAA) or spaceplanes [49], [50]. There are more than a half dozen companies attempting to build such vehicles. Some of these are designed to be single-stage-to-orbit spacecraft. Others will be suborbital spacecraft used as reusable launch vehicles. At least one other country (Germany) has a TAA development program [50]. Many companies and countries have started and abandoned similar programs during the last two decades. Until recently, the technology could not adequately sustain full-scale development efforts and the costs of research and development proved excessive. However, more than a decade of computational aerodynamics research and improvements in high temperature materials has offered hope of success and a new wave of efforts has begun. The United States is not guaranteed to be the first to develop this technology. The phenomenal growth (relative to the United States – see Chapter 10) of science and technology in Europe in the past two decades coupled with renewed interest in space promoted by the recent occupation of the International Space Station will likely cause several European programs to be resurrected. As soon as there is demonstrable success in one of the current programs, many others programs are sure to be initiated. The author expects that at a minimum, the United States, Germany, France, United Kingdom, Japan, Russia, and China would have demonstrated TAA systems within ten years of the first successes. By that time, many others including Sweden, Italy, Brazil, and Israel will have initiated development programs, if they have not already had successes.

A spaceplane is basically a spacecraft that can take off under its own power (possibly with solid rocket boosting or electromagnetic launch assistance), achieve orbit or at a minimum exit the atmosphere at hypersonic speeds (> 2 km/s), reenter the atmosphere, and land without jettisoning essential systems. Some systems would have the ability to reenter and exit the atmosphere several times without landing (possibly by refueling in space). Such spaceplanes have a number of properties of interest to the military. If they are orbital platforms, they can conduct strikes at any distance from their base. They fly at hypersonic speeds in the atmosphere. They should be able to carry significant payloads (tens of thousands of kilograms). Basically, they could be configured as extremely capable strategic bombers (carrying conventional weapons – nuclear payloads are prohibited by the Outer Space Treaty [51], although this might not stop some adversaries even if they were signatories). As a strategic bomber it might strike the most critical targets (ICBM silos, antisatellite weapon complexes, ballistic missile defense sites, and national command and control bunkers) within minutes of the initiation of hostilities. It could also strike key ports and airfields used for logistics purposes or battle groups at sea. Spaceplanes could also be used to provide rapid reconstitution of satellite constellations decimated by anti-satellite weapons. They could be used to conduct strategic reconnaissance missions swooping down at hypersonic speeds from space to extremely low altitudes to conduct ultrahigh resolution imaging and then returning to space for safe egress from hostile territory. Spaceplanes might also be used to attack an adversary's spaceplanes. The attack would likely occur in space, but the ability to change orbits rapidly (by using aerodynamic forces in the upper atmosphere to rapidly change direction without losing excessive kinetic energy) inherent in reenter-reorbit-capable platforms would facilitate intercepts.

At high hypersonic speeds TAAs would be virtually impossible to shoot down except by the U. S. National Missile Defense system or its equivalent. Given the U. S. lack of an adequate defense anywhere but CONUS and Alaska, an adversary with transatmospheric aircraft could strike any of our power projection forces anywhere in the world outside of the NMD protective shield. If the U. S. fails to deploy a comprehensive NMD system, even CONUS targets would be vulnerable.

If NPC has an indigenous aircraft or space launch industry, it should attempt to develop its own transatmospheric aircraft technology. If not, and if its economy is sufficiently robust with a strong industrial component, it may wish to start a space launch industry. The long-term future of warfare holds a major component revolving around space. With a viable international space launch industry as justification, NPC may be able to purchase one or more TAA's from other nations. NPC should examine its grand military strategy and determine which applications of TAAs can contribute most to that strategy. Among the applications that NPC may wish to develop include strategic bombing, strategic reconnaissance, and satellite replacement. An application of almost certain critical interest to NPC is defense against U. S. TAAs. Without such a capability, NPC possesses critical vulnerabilities the U. S. is certain to exploit.

The U. S. should continue to pursue research and development programs that ensure that the U. S. maintains a significant lead in transatmospheric aircraft technology. Some of this research should be aimed at determining and exploiting military applications of TAAs. Once reliable characteristics (including possible flight profiles) of such vehicles have been ascertained, U. S. ballistic missile defense programs should be tasked to determine and develop whatever modifications to their systems (if any) are needed to provide acceptable defenses against TAAs.

ATTACK BY MINES

Mines are the premier access denial weapons [52]. U. S. ships are extremely vulnerable to even the simplest mines. In past dozen years mines have been responsible for 75% of the damage to U. S. warships [53]. In April 1988 the **USS Samuel B. Roberts** *(FFG 98) struck an Iranian-planted, Russian-manufactured Type M-08 moored contact mine in the Persian Gulf [54]. The* **Roberts** *required $98 million of repairs [55]. During the Gulf War, on 18 February 1991, two ships struck mines within hours of each other [56]. The* **USS Tripoli** *(LPH 10) struck an Iraqi-planted Type M-08 moored contact mine [54], [57], [58] and was slightly damaged (it was able to remain operational and on station for 3 days until relieved). Tripoli required $3.5 million of repairs [55]. The AEGIS cruiser* **USS Princeton** *(CG 59) was damaged by two Iraqi-planted Manta bottom influence mines of Italian manufacture [58]. Although* **Princeton** *was able to restore its cruise missile strike and AEGIS air defense functions within 15 minutes of the accident [54], it ultimately required $24 million in repairs [55].*

A threatened amphibious assault on Kuwait was a diversion that contributed significantly to the success of the land war phase of the Gulf War. Had an actual amphibious landing been necessary to revive a stalled offensive farther inland, it might have become a disaster. As determined from intelligence captured after the war, the Iraqi minefields were far larger and denser than anticipated [57]. Mine clearing teams had only cleared a fraction of the known fields when the war ended. Had the assault force sailed toward the beaches, they would have encountered unanticipated minefields and suffered serious casualties.

The U. S. currently has very limited primary mine countermeasures assets. Currently, there is one **USS Inchon** *(MCS 12) class mine countermeasures support ship capable of carrying 8 MH-53E Sea Dragon airborne mine countermeasures helicopters, 14* **USS Avenger** *(MCM 1) class mine countermeasures ships, and 12* **USS Osprey** *(MHC 51) class coastal minehunting ships [59]. The MCM ships carry both minehunting (SLQ-48) and minesweeping systems (SLQ-37 and SLQ-38); the MHC ships currently carry minehunting systems (SLQ-48) although there are plans to replace this capability with a Modular Influence Minesweeping System when this latter system finishes development. With the exception of two MCM ships that are permanently forward deployed in Japan, all of the other ships are homeported at Ingleside TX. In addition there are two mine countermeasure helicopter squadrons located in Norfolk VA and Corpus Christi TX each possessing 12 MH-53E helicopters. The helicopters can carry a variety of minehunting (mine detection and location for avoidance or subsequent disposal by explosive ordnance disposal teams or minesweeping) and minesweeping (mine neutralization or destruction by intentionally and safely triggering the mine's explosive mechanism without any necessity for initial detection) systems.*

Minehunting and minesweeping are time consuming processes. Both the airborne and shipborne systems require the countermeasure platform to move at speeds much less than 10 knots. The U. S. does not possess or have access to sufficient minehunting and minesweeping assets to clear a safe path of any appreciable length for even a single carrier battle group. If a battle group faced a significant mine threat over the entire transit distance, it would be unable to arrive at its destination in the timely fashion currently demanded. If all available carrier

battle groups (CVBG) and amphibious ready groups (ARG) were sortied for a major conflict, there is only enough coverage to provide one MCM per CVBG and one MHC per ARG plus 3-4 MH-53E helicopters apiece. Mine warfare has never been very high on the Navy's priority when compared to submarines, aircraft carriers, aircraft, surface combatants, etc. It is unlikely that this will change much in the future.

Mines are sufficiently dangerous that their threat cannot be ignored, even when most evidence says that threat is phony. The possibility that one out of a hundred is real is sufficient to treat them all seriously. Thus, even a few fake floating mines spread in the path of an oncoming carrier battle group will cause it to slow down and convert to a mine avoidance mode of advance. The use of fake mines also poses virtually no risk to those who deploy them. Since their use is no more than a harassing tactic, it poses little likelihood of escalation. Use of fake mines might even be considered a viable tactic during peacetime to discourage U. S presence.

A number of improvements can and probably will be made to mine technology. Smart mines can wait for precise combined acoustic, magnetic, and pressure signatures giving them the ability to attack only the highest value targets. Mines can be strewn throughout the world's oceans, remaining inert (and probably undetected) until remotely activated in times of conflict. U. S. harbors might have already been sown with remotely activated mines by foreign commercial ships, and we would not know it until a conflict broke out or an accident of some sort (such as being caught in the nets of a fishing trawler) betrayed their existence. Self-propelled mines (essentially remotely-fired torpedoes) do not have to be collocated with their sensors. Such mines might be hidden in shoal waters where minesweeping or hunting would not be thought necessary, with tiny sensor packages located miles away at the bottom of navigable passages. An acoustic modem could be used to trigger the mine to activate and home on the target, when an appropriate target was detected. The small, bottom-lying sensor packages would be difficult to detect and locate by any current mine warfare technology with the possible exception of marine mammals.

By combining underwater missile launch technology with smart mine technology, it is possible to create sea mines with effective chemical and biological weapon capabilities. On detection of the appropriate class of ship, the chem/bio mines would release a launch capsule capable of projecting a chem/bio bursting munition several hundreds meters into the air directly over the target ship. The chem/bio agent would disperse and be drawn into the target ship's interior before any chemical/biological defense condition could be established. If the collective protection system was already activated and the ship buttoned up, at a minimum, the agent cloud would thoroughly contaminate the exterior before the washdown system could be activated. At worst, many members of the crew would be adversely affected by the consequent cleanup/decontamination required. See Appendix A for illustrations of these devices.

Presently the operational Navy appears to be moving towards more reliance on minesweeping than minehunting, although minehunting R&D remains strong. This adds to our vulnerability to mines, because there are a variety of techniques that can defeat minesweeping. For example, counters can be used to wait until a preset number of trigger signals (each signal supposedly coming from a separate valid target) is reached. Thus the mine will not deto-

nate when the first N-1 targets pass by, but wait for the N^{th} target. A minesweeper must properly simulate a real target N separate times (with a time delay between each simulation) before the mine will be swept. Of course N will never be known in advance and each sweep adds to the time required for clearance. Fortunately, unless employed against commercial shipping, the number of high value targets (major warships) that will pass by the mine will be small and the enemy must choose N accordingly. Another counter-countermeasure is to increase the number of signatures (or influences) that must be matched for a valid target to be declared. These influences may include very sophisticated acoustic signature matching, pressure profile matching, and magnetic signature matching, as well as more exotic signatures such as opacity to cosmic ray muon flux (wood and fiberglass hulled mine countermeasures ships will not attenuate the muon flux as much as an metal-hulled aircraft carrier) or requirement for simultaneous presence of multiple matched acoustic signatures (carriers always have destroyers nearby; minesweepers do not). Remote activation can also negate minesweeping. If surveillance can provide precise information as to when high value targets will pass by a mine or minefield, the mines can be activated only at the proper time. They can be dormant while any minesweeping is taking place (which may also be determinable from the surveillance assets).

NPC should invest in offensive mine warfare technology. Although it should not neglect shallow-water mines and surf-zone mines, it should place special emphasis on mines that are functional in waters deeper than 30 meters (the goal of an access denial system is to prevent the enemy from getting close to the beaches). It should especially emphasize the ability to use commercial vessels and submerged submarines to covertly accomplish its minelaying. It should pursue the development of smarter, more lethal mines and mines that can be remotely actuated. Any mines developed for deployment outside of NPC's territorial waters should possess either remote or automatic disarming or self-destruction capability. The goal of mining is to harass a specific enemy; it is not to draw the wrath of every nation relying on commercial shipping for its economic health. It might be cost effective to provide these mines with a remotely actuated beacon to facility their recovery (and reuse) after employment in an operation.

NPC should invest in minehunting and mine sweeping technologies as the U. S possesses a number of aircraft-deliverable and submarine-deliverable mines and has been known to mine the harbors of its adversaries. If consistent with its chemical/biological warfare policy, NPC should develop sea mines with chemical, biological, or radiological warheads. NPC should also consider the acquisition of a number of fake mines of indeterminate origin. Fake mining of certain shipping lanes might provide NPC with a significant economic advantage over some of its competitors (NPC ships' captains would know the mines were fakes and could deliver the goods on time, whereas competitors would not and could not). If enough fakes are discovered, then concerns about mines will diminish, making real mining substantially more effective when it is actually performed.

The U. S. Navy should significantly improve both its minehunting and its minesweeping capabilities. Both kinds of capabilities need to be available for static (clearing harbors, channels, and chokepoints) as well as in-stride operations (transit). Mine detection sonars (or other mine location sensors) should be considered for deployment on combatant and combat auxiliary ships of all classes. In-stride mine-

sweeping capabilities should be considered for deployment on all destroyers and cruisers. Aircraft carriers and amphibious ships should have airborne minehunting and minesweeping platforms in their aviation complements. The Navy should consider the development and acquisition of new classes of dedicated mine countermeasures ships, in order to free our limited numbers of combatant ships for performing their primary duties.

The U. S. may wish to consider supplying minehunting and minesweeping equipment to the U. S. Coast Guard. This would facilitate the protection of critical ports, naval bases, and coastal waterways. Mining U. S. waters used for logistics will likely prove to be as effective in helping to establish an access denial capability as mining the littoral waters to which access is to be denied.

Consideration should also be given to innovations in ship design. Incorporating armor, structural strengthening, and advanced damage control technologies into the next generation of ship designs may make them less vulnerable to destruction by naval mines. Despite damage, the new ship designs may be able to continue to function and even fight for extended periods of time. Any damage limitation that new designs can provide will reduce the costs of repairing mine damage.

ATTACK BY ADVANCED TORPEDOES

Most naval vessels lack not only the ability to detect an attack by torpedoes (especially those of the wake-homing variety) but also lack any effective defense even if an attack is detected. Most current defenses use decoys to draw the torpedoes away from the true target. Current surface ship decoys are usually towed and can only be employed if the target ship is underway and in relatively deep water (nominally several times the ship's draft). As decoys improve, the seekers on torpedoes will also improve. It should be relatively easy to design a multi-signature seeker that could easily distinguish between a decoy and a real target, especially during the endgame. Decoys have another disadvantage. If they are not sufficiently real to cause the torpedo to detonate on closest approach, the torpedo may realize that it has lost track and attempt to reacquire the original target or an alternate target. A protected ship may inadvertently cause the destruction of an unprotected ship.

A second type of defense is to shoot the "archer" before he has a chance to fire his torpedoes. This is a primary reason that nuclear attack submarines are attached to carrier battle groups, yet the development of very long-range torpedoes (>100 km) makes it less likely that we can detect the launching platforms in time. Wake-homing guidance permits the firing of torpedoes at ranges beyond which targeting data adequate for conventional guidance can be acquired. Mere knowledge of the presence of naval forces in an area is adequate. Torpedoes can be fired in the general direction of the targets; the torpedoes then autonomously acquire the wakes and follow them to the present target locations.

The United States is developing a defensive capability against torpedoes [60], however, it will probably be of limited effectiveness and require the ship to perform maneuvers that disrupt normal operations. If the U. S. should develop an effective anti-torpedo torpedo (analogous to an anti-missile missile) and an all-aspect torpedo detection capability, then this vulnerability would be significantly reduced. However, it is not clear that the U. S. could afford to place such complex protection systems on every class of ship. The loss of the unprotected ships would require other ships to perform the mission functions of the lost ships as well as their own mission functions. This would clearly reduce the overall effectiveness of any battle group.

The performance of an anti-torpedo torpedo defense system will likely have a strong dependence on torpedo speed and on torpedo endgame kinematics. A system that can reliability intercept 60-knot torpedoes may be ineffective against 100-knot or 300-knot torpedoes. In principle it is possible to propel a torpedo at extremely high speeds. The practical limitation is range. It takes considerably more fuel expenditure to travel one nautical mile at 100 knots than it does to travel one nautical mile at 50 knots. For a given quantity of fuel, the range will vary nominally as the inverse square of the speed. In fact the need for larger engines to burn the fuel at faster rates, causes the range (vs. speed) to drop even faster than inverse square law. However, if the high speed is needed only during the last few thousand meters, the 10-20% reduction in maximum range might be acceptable. The increased kinetic energy that a high-speed torpedo possesses may give it additional lethality if ship designers add increased "armor" (such as double hulls) for passive torpedo defense.

A torpedo that performs moderately violent maneuvers during its terminal guidance phase would be much harder to intercept than one that travels in straight lines. Inclusion of a maneuvering capability or a high-speed sprint capability requires only moderate increase in torpedo design complexity, but would significantly degrade the capabilities of any torpedo defense.

NPC should ensure that it has an adequate long-range (>100 km) torpedo capability in its force structure. These torpedoes should have wake-homing, inertial, as well as acoustic terminal seeker guidance. The seekers should be designed to be immune to current anti-torpedo decoys. The torpedo attack capability should also be provided to combatants other than submarines. At a minimum, some patrol craft and long-range aircraft should have torpedo attack capabilities. Employment of torpedoes in conjunction with mines, cruise missiles, ballistic missiles, aircraft, and surface vessels in an attack will enhance the overall effectiveness. Having to fight one threat always detracts from one's ability to fight a second (or third or fourth) threat. NPC should strive to exploit every weakness of the United States if it is to be successful in its access denial mission.

NPC should follow U. S. development efforts in torpedo defense. As decoys are improved, seeker designs should be improved accordingly. If the U. S. develops anti-torpedo torpedoes, then NPC should improve its torpedoes to reduce the effectiveness of the defenses. NPC designers should consider incorporation of maneuvering and high-speed sprint capabilities. Conversely, NPC should consider development of torpedo defenses for its own naval assets. Submarines are a major component of U. S. anti-surface and anti-submarine warfare capabilities. The ability to defend NPC submarines and surface ships against U. S. torpedoes would significantly alter the balance of power.

The U. S. needs to develop improved defenses against torpedoes. New active decoys should be designed to seduce torpedoes with probable more modern seeker designs. Consideration should be given to incorporating decoys into autonomous unmanned vehicles that could be used as escorts when underway, as screening "vessels" when loitering in littoral waters, and as propelled decoys when under actual attack. The latter mode might utilize a yet-to-be-developed wake-generating decoy useful against wake-homing torpedoes. Decoys will never provide complete protection. Recognizing this, the U. S. should develop anti-torpedo weapon systems. These might be anti-torpedo torpedoes fired along bearings determined by torpedo detection sonars. They might consist of torpedo-sensitive mines delivered by mortars fired along bearings determined by torpedo detection sonars or anticipated directions of attacks (if bearing data is unavailable). They might consist of explosive projectiles fired from guns (which are pointed by sonar analogs of air defense radars). Consideration should also be given to incorporating armor and other survivability design features into the next generation of ship designs.

ATTACK BY ADVANCED NON-NUCLEAR SUBMARINES

Virtually no maritime force in the world today possesses the ability to reliably detect, track, and engage submarines in littoral waters. Non-nuclear, electric-drive submarines are virtually undetectable in this environment even when they are moving. A substantial fleet of air-independent-propulsion submarines with the ability to stay submerged for weeks in littoral waters would provide a definitive capability to deny littoral waters to any naval force including a nuclear attack submarine fleet [61].

A number of developing technologies may provide significant changes in submarine philosophy and design. The continued advances in high-temperature superconductor technology may ultimately permit the incorporation of superquiet magnetohydrodynamic propulsion. Increased automation of ship's function coupled with increased reliability of that automation could result in large reductions in required manpower. This in turn could result in much smaller submarines. Smaller submarines will use less power to maintain desired speeds and can remain submerged longer for a given quantity of fuel, possibly rivaling nuclear submarine submergence times. The development of non-nuclear submarines with the speed, depth, and endurance of nuclear submarine capabilities as well as electric-propulsion quietness would give the nation that possessed them a global subsurface warfare capability that would be nearly unstoppable. Not only surface ships but also our attack submarines and ballistic missile submarines would be at risk from the instant they cleared port. This too would cause naval strategy to be revised in fashions that can only enhance an adversary's access denial capability.

The ultimate in reduced manpower is the unmanned submersible. Unmanned underwater vehicles can be made very small and exceedingly quiet, yet they can travel substantial distances at modest velocities and remain submerged for periods considerably longer than a diesel submarine. Weapon for weapon they would be much cheaper than manned submarines and being unmanned could be considered expendable (although there is no reason they should not be recoverable). If artificial intelligence comparable to that discussed in the next section on unmanned aircraft were available, then there is every reason to expect that a submarine comparable to a modern manned submarine could be obtained in a platform with one-quarter to one-third the displacement of the manned platform. Cost would be comparably smaller. The lack of crew might permit such a platform to dive to depths of thousands of meters and open up new avenues for attack of both surface and subsurface targets. Even lacking artificial intelligence, several much smaller unmanned platforms operated from a manned submarine via fiber-optic links or acoustic modems could increase the attack options, make adversary defensive measures more difficult to implement, and increase the host platform survivability.

NPC should buy or steal the best submarine technology from around the world. It should use this stolen and/or purchased high technology to augment and enhance its current non-nuclear submarine building programs. The primary goal is to develop a fleet of ultraquiet, long-endurance, coastal submarines (SSKs) that can keep U. S. attack submarines at least 500 nmi from NPC's shores. NPC should procure a substantial submarine fleet. If possible, at least two different designs should be procured to prevent any single vulnerability from rendering the entire fleet at risk. NPC should have sufficient boats to observe regular training and maintenance regimens, to thoroughly patrol all NPC littoral waters, and to be able to sortie multi-boat wolf-packs to every shallow water choke point on the approaches to NPC coastal waters.

A long-term goal is to develop ultraquiet non-nuclear attack submarines capable of global reach. Bearing in mind that such developments may not be ready until 2030 or beyond, NPC should not neglect nuclear attack submarines (SSNs). A fleet of a half-dozen or more SSNs will serve to keep U. S. attack submarines tied up in blue water away from the fleets and away from areas where they can perform their traditional intelligence & warning roles. If available in sufficient numbers some of the SSNs should be used to provide escort defense for NPC's ballistic missile submarine fleet. However, NPC should attempt to develop non-nuclear replacements for the SSNs as soon as the developing technologies permit, unless breakthroughs in reactor quieting occur.

NPC should also consider developing unmanned submersible technology. Such devices could provide stand-alone systems for conducting dangerous yet typically uninteresting missions such as picket duty. They can also provide increased numbers of combatants at little additional cost by operating them as adjuncts to more conventional manned submarines.

The U. S. needs to develop improved sensor technologies for detecting extremely quiet submarines in both littoral waters and the open oceans. These might be based on novel sonar concepts, more sensitive magnetic detection arrays, laser backscatter sensing, or some other technology. New weapons may need to be developed to exploit the new sensor systems. Regardless of the types of sensors and weapons, both need to be deployed in adequate quantities in the theaters where the submarine threat is being faced.

An old saying goes, "it takes a submarine to kill another submarine". Since our SSNs are vulnerable in littoral waters given the postulated advanced threat, the U. S. might consider developing a new class of small, non-nuclear attack submarines designed explicitly for littoral submarine warfare. These submarines might be carried to the theater of operations by a tender or mother ship (to prevent any need for extended cruising) and deployed only when entering regions of increased threat. These small attack subs might even be remotely piloted (and thus, unmanned). The U. S. should also consider developing or purchasing a few advanced non-nuclear submarines comparable to the adversary's, if only to have realistic targets against which to practice new detection and engagement techniques. If enough of these were purchased, they might provide an interim capability against the adversary's submarines until better solutions are found.

For the same reasons that NPC should consider developing unmanned submersible technology, so should the United States. The ability to use these devices as scouts for the SSNs would greatly enhance combat coverage in littoral environments and improve survivability as well.

ATTACK BY UNMANNED AIR SUPERIORITY VEHICLES

Manned aircraft suffer a fundamental limitation of not being able to sustain accelerations greater than 10 g due to the physiological limitations of human pilots [62]. It is possible to design an aircraft to sustain much higher g loads than 10 g. Accelerations of 20 g, 30 g, or higher are possible, although as g-loading increases, more weight must be dedicated to structure at the expense of fuel or payload. This penalty is partially mitigated in an unmanned aircraft because no resources need to be dedicated to the crew's cockpit, controls & displays, ejection system, and life support system. An unmanned, supersonic aircraft capable of 30 g maneuvers and loaded with appropriately-advanced weapons, would not only be able to easily outmaneuver and shoot down any manned aircraft the U. S. has conceived, but also be capable of evading every air-to-air and surface-to-air missile on U. S. drawing boards. "Pilots" at remote consoles could provide mission control over wideband data links.

A common rule of thumb used by missile designers is that an interceptor missile must have at least three times the acceleration (g) capability of the target it is trying to intercept. <u>See Appendix F for a technical discussion on the 3x acceleration heuristic.</u> ***Anti-aircraft missiles typically have 30-50 g capabilities to permit intercept of manned aircraft. Such g capabilities are also adequate to intercept most cruise missiles as these targets seldom have high g capability. However, against an unmanned aircraft with 30 g capability, 30-50 g interceptor capability is not adequate. Any intercepts achieved would be due to random chance or "remote pilot" error. A single squadron of unmanned air superiority aircraft could conceivably defeat 4-16 times as many manned fighter aircraft, depending on the number of weapons each unmanned aircraft could carry. It is only a matter of time before manned aircraft become obsolete.***

By 2020 it may be possible to replace the remote "pilots" by artificially intelligent autopilots. In 2020, personal computers may rival the human brain in memory and processing power (this is an unequivocal prediction of Moore's Law, if that law remains valid for the next 20 years – it has been valid for the last 35 years) [63]. The major uncertainty is whether or not the software needed to exploit that processing capacity and provide acceptable artificial intelligence will be available. Absence of pilot equipment requirements may allow unmanned aircraft to be somewhat smaller and cheaper than their manned counterparts. Loss of an unmanned aircraft will be much less significant than the crash of a manned aircraft. Even if the "pilot" cannot be eliminated, remote control of unmanned aircraft could be delegated to enlisted personnel rather than officers, resulting in reduced manpower costs. Lastly, in the first major battles between manned and unmanned aircraft, the psychological impact on the morale of the aviation community caused by massive losses of trained pilots at the hands of unmanned killing machines could be as staggering as the losses themselves.

The same artificial intelligence that permits the development of UASVs will also permit the development of unmanned combat platforms of all kinds. Robotic tanks and unmanned submarines present distinct advantages. Foremost is the potential reduction in friendly casualties that will ensue by removing personnel from direct combat. However, most of these other

unmanned platforms do not present direct performance advantages as overwhelming as elimination of the "10 g" acceleration limitation.

NPC should take the lead in developing unmanned air superiority vehicles (UASV). It would revolutionize the field of air combat. Most other countries will be quick to follow NPC's lead. However, the first country to field viable UASV could name its own prices and would capture a large share of an entirely new military market. Unfortunately, the author anticipates that the United States will not be able to catch up quickly because its aviation communities dominate both the Air Force and Navy and those communities are governed by the "silk scarf" phenomenon (if you aren't a fighter pilot, you aren't a real pilot). Few members of these communities will willingly relinquish their places in the cockpit to a computer or a communications link.

NPC should emphasize development of the software necessary for an artificially intelligent autopilot. If desired, it can delay the development of the unmanned airframe until later in the game (or until another competitor announces its efforts in this arena). There is no magic in designing an agile, supersonic, unmanned aircraft. It hasn't been done before because "airplanes must have pilots!" The money saved by substantially reducing the ranks of officer aviators and building cheaper UASVs can be used to purchase more UASVs or to permit more training time for the enlisted operators. It is expected that NPC will also follow the general worldwide trend in using unmanned vehicles for non-glamorous missions such as reconnaissance, surveillance, targeting, or even precision strike. The spin-offs from the unmanned air superiority program will make performance of these other missions extremely cost-effective.

The U. S. needs to begin to make plans for a future in which manned aircraft are obsolete. Despite any potential opposition from the aviation (pilot) community, the U. S. needs to undertake development of unmanned air superiority vehicles. Such projects can build on the significant efforts currently underway addressing unmanned reconnaissance and combat air (strike) vehicles. Emphasis should be placed on both high-g, long-endurance airframe design and on the development of an "artificial pilot" using the latest in advancing computer and software technology. Concurrent with aircraft design activities, the U. S. should pursue advanced interceptor missiles. Given the "3x acceleration" heuristic used above, the interceptors should be capable of at least 100-g maneuver capability with speeds in the Mach 3-5 regime, ranges in excess of 50 km, and hemispherical seeker coverage. When coupled with improved fire control technology these new interceptors would provide current aircraft with acceptable kill probabilities against adversary UASVs as long as those UASVs are not allowed to close to dogfight distances. This will require the ability to shoot beyond visual range. Development of a non-cooperative target identification capability will be the key to permitting engagements without "visual identification" of the target.

ATTACK BY INFRARED ANTI-AIRCRAFT MISSILES

U. S. fixed wing aircraft routinely carry integrated radar warning, radar jamming, and chaff dispensing equipment. Few if any of these same aircraft carry any infrared countermeasures beyond flares occupying a few slots in the chaff dispenser. Improved infrared flare designs have proved remarkably versatile in providing counter-counter-countermeasure capability against almost every infrared seeker counter-countermeasure. However, the next generation of anti-aircraft missiles will include a large number of examples employing infrared imaging in multiple spectral bands for almost complete immunity to flare (and most other infrared) countermeasures. Even the most advanced flares will be useless against these missiles. The generation beyond that (available in 2020 time frame) will integrate both RF and IR capabilities with extremely robust target detection, recognition, identification, and tracking capabilities, as well as possessing extremely high speed (>Mach 4) and agility (>60 g). These missiles will also be capable of detecting the infrared skin emissions of stealth aircraft and attacking them, if adequate warning and cueing can be provided from other sources for the missiles to be initially launched in the right direction. Aircraft without sophisticated "dc-to-light" electronic warfare capabilities will not be able to defeat the threat posed by these missiles.

Electronic warfare has consistently been the odd man out in funding skirmishes ever since the field was invented. Nothing is likely to alter this trend. Even the most advanced electronic warfare concepts under examination will not completely counter the threat of the generation-after-next missiles. Directed energy weapons will handle the coming threat, but these are likely to be too large for inclusion on small mobile platforms such as aircraft. Consequently, without new developments in infrared electronic warfare our aircraft may find themselves increasingly threatened.

The new generation of missiles will also be quite effective at attacking and destroying cruise missiles, negating one of our major means of land attack. Employment of antiradiation missiles against the new air defense threat will be of decreasing effectiveness as the new threat will increasingly rely on non-radiating means of targeting, such as infrared search & track or multistatic radar systems. Some variants of these missiles could possess over-the-shoulder air-to-air firing capability (made possible by computer-controlled stability at angles of attack greatly exceeding ninety degrees). Others with very sophisticated IR imaging seekers will be able to pick out a desired enemy target from the middle of a "furball" of friendly forces engaging adversary forces, without external designation by the operator or lock-on-before-launch. See Appendix G for a detailed discussion of missile guidance technologies. ***The ability to fire into an ongoing air battle from the outside, lock on and kill only hostile aircraft, and not produce fratricide will also have a significant effect on air warfare. Air cover will no longer need to be kept outside the engagement envelope of air defense weapons. It can continue to engage the enemy even as the air defense missile systems begin to become effective. Pilot workloads will also go up dramatically as they must now cope with additional threats simultaneously with their other functions.***

NPC should make sure that it purchases, or even better, develops the best infrared anti-aircraft missiles of the generation after next, in sufficient quantities to make U. S. air superiority a questionable proposition at best. It should develop the basic technologies (infrared detectors, multiplexers, array processors) that will make possible multispectral imaging infrared seekers with extremely high image resolution, simultaneous imaging in multiple spectral regions, and automatic target recognition-based processing. Such seekers with the ability to intelligently detect and identify targets will permit lock-on-after-launch operation as well as firing into a crowd. On-board automatic target recognition will require NPC to develop extremely powerful, compact, data processing systems and software to accompany them. Such powerful systems will find applications in many other weapons such as anti-ship missiles, unmanned air superiority vehicles, anti-satellite missiles, and space-based surveillance systems. NPC should also attempt to develop compact radar seekers and develop the technologies to integrate the radars and infrared seekers into true dual-mode seeker systems.

To exploit the capabilities of these seekers NPC should pursue the development of advanced missile airframes. These airframes should be faster than any target they are designed to attack. They should have the ability to pull at least 3x the g-levels of their intended targets. This may require advanced thrust vector control. They should have operational ranges in excess of the missiles of the intended adversary (the U. S.?). They should be stable at angles of attack in excess of ninety degrees (i.e., flying backwards). This will certainly involve intelligent computer controlled stabilization and may require innovative aerodynamic shapes. NPC should procure enough of these advanced airframes and seekers to completely replace all of its older generation surface-to-air and air-to-air missiles and to provide enough weapons to arm all appropriate platforms for an extended war of attrition.

The U. S. should continue its efforts at developing advanced imaging infrared guided missiles. These will prove essential in attacking adversary targets employing stealth technology. Anticipating an adversary's development of similar missiles, and recognizing the intrinsic decoy (flare) immunity of the next generation of missiles, the U. S. should develop infrared laser-based countermeasures capable of jamming (blinding) the advanced imaging seekers by damaging the infrared detectors. This will require development of multi-wavelength, moderate average power, infrared lasers. The U. S. should pursue innovative gas laser techniques as well as solid state approaches. The U. S. has neglected military gas laser research for many years without having achieved any of the supposed benefits of solid state lasers. There is reason to expect that new gas laser designs can provide higher output powers at higher efficiencies and lower costs in comparable package volumes as those achieved by solid state lasers.

CHAPTER 5. COUNTERS TO OFFENSIVE SYSTEMS

RELIANCE ON STEALTH

The United States is spending a large fraction of its defense budget to acquire platforms with reduced observables (stealth) [64]-[66]. See Appendix H for a technical discussion of stealth. ***There are four basic problems with design for stealth. First, stealth is expensive. Every aspect of exterior design must be meticulously controlled and special materials must be employed. Second, stealth is difficult to maintain. Modifications to a platform's exterior, corrosion, aging, or weathering of external materials, sloppy maintenance, failure to properly close all external doors/hatches/panels after opening for operations or maintenance, failure to stow supplies, equipment, & tools, and opening of doors and hatches for normal operations can significantly increase the detectability of a platform. Third, stealth is a moving target. Acceptably low signature levels at one time may not (and probably will not) remain acceptably low in the future. Advances in component technology, packaging, or signal processing permit significant advances in detection capability for seekers of the same basic type. Furthermore, stealth in one signature does not imply stealth in other signatures. A platform designed for low radar cross section may be undetectable to a conventional scanning radar seeker. However, if the seeker technology changes to use synthetic aperture radar, the low cross section may not prevent detection at useful ranges, because synthetic aperture radar relies on image contrast for detection, not threshold exceedance. Similarly, if a platform designer designs for low radar cross section, his design may be detectable by passive infrared seekers. If he also controls the infrared signature, the platform may be detectable by laser radar seekers. If he also controls the laser signature, the platform may be detectable by visual (television) seekers and so on. Fourth, stealth is most effective at protecting against the first hit. If by pure accident or use of a counterstealth seeker a single missile strikes a stealth ship, the damaged ship's signature will increase dramatically. The "hole" in the exterior, structural deformations, and dislodged radar absorbing materials will serve to increase radar cross section significantly. Smoke and fires will increase the visual and infrared signatures significantly. The noise associated with damage control efforts will hamper any attempts to be acoustically silent. Once a stealth ship is hit the first time, it is much more vulnerable to subsequent hits, even by less capable threats. Each successive hit will make the situation worse.***

It is not difficult and only moderately expensive to significantly reduce the signature of a target. It is very difficult and prohibitively expensive to reduce the signature to effectively undetectable levels (levels so low that the target return becomes comparable to background clutter or noise). The more signature elements which must be controlled, the more expensive will be the resulting design. The high cost of stealth leads the U. S. to buy fewer platforms for an enemy to be forced to defeat. Countering only the conventional radar and infrared threats made the B-2 bomber prohibitively expensive (at last count we had procured a total of 21 aircraft at an average cost of $2.1 billion each) [67]. If low- or moderate-cost counter-stealth systems can be developed, and our high-cost "invisible" platforms suddenly become "visible", then stealth will become a bad investment for the U. S. to have made. Even the B-2 stealth

bomber is not undetectable; an ABM-quality phased array radar operating at megawatt average power levels would be capable of detecting the B-2 at ranges capable of allowing intercepts. However, in most cases it would not be cost-effective to deploy such radars against the limited B-2 threat. Even the best stealth designs cannot eliminate all possible signatures. Some kind of sensor or another will be able to detect and track them. It is merely a matter of finding the right sensors or combinations of sensors that can be acquired and fielded at reasonable cost to exploit this vulnerability.

Finally, stealth is not a viable defense against all threats. A stealth aircraft on the ground at an airfield is just as vulnerable to an air strike with cluster bombs as a non-stealthy aircraft. A stealth warship tied up to a dock in a friendly port is just as vulnerable as a conventional warship to destruction by a terrorist truck bomb or by a limpet mine emplaced by special operations forces. That same stealth warship might be relatively immune to cruise missile attacks, but is highly vulnerable to damage from medium anti-tank missiles fired at point blank range by a crew member of any of the thousands of small fishing and trading boats from dozens of nations that frequent the littoral waters. It would cost very little to provide infantry anti-armor weapons to several hundred "fishing boats" crewed by reservists and flying a false flag. Random chance encounters would provide the targeting that millions of dollars of stealth was designed to avoid. Small arms fire was responsible for downing a number of strike aircraft during the Vietnam War. A jet flying into a "wall of lead" may be destroyed whether or not any gunner ever saw the aircraft. Mere knowledge that an aircraft was in the vicinity was sufficient to trigger the response. If the probable targets, probable routes of attack, and likely times of attacks can be established in advance (this is occasionally relatively easy to do), asymmetric defense against even stealth aircraft becomes simpler. All the preceding examples highlight the hard truth: the advantages of stealth can be defeated by asymmetric attacks.

NPC should devote significant research and development into counter-stealth technology. If a breakthrough is made, it will negate one of the few true advantages that U. S. forces possess and turn that advantage into a liability. Specific technologies that should be investigated include improved infrared search & track sensors, coherent laser radars, impulse radars, netted atmospheric acoustic sensors, magnetic sensors, gravitational sensors, and netted multistatic radars. NPC should not neglect the possibilities that may accrue from using large numbers of low-cost, modest-performance sensors networked with massive data processing (the U. S. sound surveillance system – SOSUS – is essentially a system of this type). To facilitate development of counter-stealth systems, the NPC intelligence services should make acquisition of stealth technology data one of their highest collection priorities. NPC should incorporate this stealth technology into its systems wherever it is cost effective. However, it should avoid an over-dependence on stealth to be able to accomplish any mission. Self-defense equipment and weaponry should not be neglected. The U. S. may well develop its own counter-stealth systems. NPC intelligence should also make every attempt to gain access to U. S. developments in this area.

NPC should determine which U. S. stealth assets pose the biggest threat to its access denial capabilities. Asymmetric strategies should be developed to neutralize these assets. Multiple strategies are desirable as any asymmetric strategy may work only once and may not neutralize all of the U. S. assets. Special attention should be given to exploiting the signatures that the stealth design did not principally address. Stealth platforms generally rely on special conditions to enhance their survivability. For example, the B-2 flies at night. NPC should examine whether there are technologies that might alter those special conditions and temporarily create conditions advantageous to the defense. In the B-2 example, perhaps an artificial twilight could be created that would silhouette the black aircraft against the suddenly bright sky.

The United States should take a more balanced view towards stealth. It should recognize that stealth is neither invincible nor a panacea. Effective undetectability is not likely to be achievable; or if it is then its effectiveness will be short-lived. The United States should incorporate only that level of stealth that can be economically accommodated. This possibly less capable level of stealth should be balanced by enhanced protective design features, self-defense weaponry (hard-kill and soft-kill), and increased numbers of platforms (made possible by reduced costs). Given its current commitment to stealth in a number of platforms, the United States should invest in counter-stealth technology development. This will provide early warnings of where weaknesses have developed with respect to our stealth platforms and permit new tactics or missions to be devised that will take advantage of the platforms' capabilities without forcing them to confront the adversary when they are most vulnerable. It will also permit our own defenses to detect and negate any stealth platforms an adversary may be developing.

JAMMING OF GPS AND GPS-DEPENDENT SYSTEMS

To save money the United States has committed to making almost every precision-guided weapon and delivery platform dependent on GPS [68] for required accuracy. See Appendix G for a detailed discussion of the GPS system. ***In some cases, guidance accuracy is provided only by the GPS system with no backup. In addition, the civilian sector around the world has jumped on the GPS bandwagon to permit precision navigation in high-density, confined air and sea corridors. It has been demonstrated that current GPS-based systems are susceptible to "$500-dollar" jamming systems made from Radio Shack parts [9, 10]. Although improvements are planned to overcome the current susceptibility, it is likely that "five-thousand-dollar" jammers made from more powerful components will be capable of jamming even the improved GPS. Improvements in computer technology may even make it possible to deceive or spoof GPS guidance systems into hitting the wrong targets. GPS jamming on the U. S. or European home fronts could cause severe problems in air and sea transportation. Jamming in San Diego, Long Beach, Seattle, Norfolk, New York or any other major harbor would cause ship traffic to revert to older radar-based navigation. A two-fold reduction in traffic throughput (due to increased ship spacing and reduced ship speed) would be a minimum result. GPS jamming coupled with conventional radar jamming in the English Channel would inevitably result in collisions, sinkings, oil spills, and general economic chaos.***

NPC should make every effort to develop and deploy powerful GPS jamming systems. These jamming systems should be deployed to protect all high value target areas. They should also be deployed with all stationary or slow moving forces. A strategy should be developed as to how to employ GPS sabotage to maximum effectiveness. Multiple jamming systems should be covertly deployed to every major U. S. military and civilian port. Use of these covert systems should be coordinated with the overall NPC war plan and timed to produce maximum disruption. If possible the covert jammers should be located on mobile platforms to make it considerably more difficult for the U. S. or its allies to radiolocate and destroy the jammers. NPC should obviously refrain from making any use of the American GPS system for its own purposes.

The advantages of a "GPS" are large enough that NPC should develop and deploy its own system using technology sufficiently different from the U. S. that a copycat jamming approach will not be effective. Such a system might employ only a regional-coverage satellite constellation or a small satellite constellation combined with a number of fixed surface emitter sites. NPC should avoid making the mistake of over-relying on its own "GPS" and should include adequate backup guidance (inertial and/or terminal guidance) in all of its weapons and platforms.

NPC should also consider targeting U. S. GPS satellites with any anti-satellite systems they may develop. If 25% or more of the constellation is destroyed, then navigation performance will become sporadic (the likelihood of having four satellites in view will be significantly reduced). It will take months for the U. S. to restore complete GPS capability. Targeting the GPS satellites might be considered more defensive in character and thus less provocative than targeting communications or intelligence satellites.

The current GPS system should be improved to reduce its jammability. New satellites should be considered which are designed to radiate considerably higher average powers over considerably wider bandwidths (using spread spectrum transmission). Receivers should incorporate antennas capable of generating multiple nulls that can be placed at angles of suspected jammers. More satellites operating on differing frequencies could be placed into the constellation making it easier for a receiver to find four unjammed satellites.

Nevertheless, the U. S. should place less reliance on GPS for both navigation and guidance purposes. Navigation systems should take advantage of dramatic performance improvements and cost reductions in inertial guidance sensors. Coupling a quality inertial guidance system with GPS would provide precision backup for brief periods when GPS might be effectively jammed. Some guidance systems can make similar use of coupled GPS-inertial navigation. However, the potential for targets to be increasingly mobile cannot be solved by inertial navigation adjuncts. Research and development needs to be continued in terminal seekers capable of autonomously detecting, identifying, and tracking specific targets while remaining affordable in cost.

JAMMING OF PRECISION-GUIDED WEAPONS

Smart weapons [69]-[71] present a highly cost-effective alternative to dumb weapons. It is possible to take out a bridge or bunker with a single precision-guided weapon dropped from a single airplane without suffering any casualties. Destruction of the same bridge or bunker might require dozens of sorties dropping hundreds of dumb bombs at a cost of a dozen aircraft lost. Because of this, the United States has traded away ownership of large quantities of dumb weapons for limited quantities of extremely high precision weapons. As mentioned in the preceding section, many of our newest surface attack weapons use GPS for precision guidance. In addition to using GPS for guidance, the U. S. possesses several other kinds of precision-guided weapons. See Appendix G for a technical discussion of missile and weapon guidance techniques. ***Foremost among these are laser-designated bombs, missiles, and artillery shells. A handful of other precision weapons rely on image-based guidance. The overwhelming dependence on precision-guided weapons leads to a foreseeable (yet infrequently considered) vulnerability. That is, any precision-guided weapon can be jammed. The fundamental tenet of electronic warfare is: "For every measure, there is a viable countermeasure." In fact, it is not terribly difficult to jam most precision-guided weapons.***

High-pulse-rate laser emitters can jam the seekers on laser-guided weapons. These emitters can be packaged as expendable laser jammers or as permanent platform protection assets. Had Iraq possessed such devices, the wonderful news pictures of airborne infrared images of bunkers and buildings being destroyed by bombs and missiles would never have been available. Wire-guided, fiber-guided, or beamrider missiles constitute another major class of weapons. Jamming or attacking their fire control units can effectively negate these systems. As these are invariably electro-optical sensor-based, electro-optical jamming systems would be required. This jamming technology has been available for many years, awaiting a suitable threat to justify its deployment. A third class of systems uses imaging sensors as the main component of homing seekers. High intensity light sources (including lasers) can be directed at these seekers to jam or even damage them. In general, almost all of the United States precision-guided weapons can be jammed by electronic warfare systems of no higher than medium complexity. Effective jamming of precision-guided weapons can reduce their effectiveness to levels far below those of unguided weapons. In effect our entire arsenal of precision-guided weapons could be rendered less effective than an arsenal orders of magnitude larger containing only unguided weapons.

Similar comments can be made about cruise missiles and anti-aircraft missiles – both types of missiles are also precision-guided weapons. Both cruise missiles and anti-aircraft missiles can also be jammed. Most cruise missiles use active radar guidance and any kind of radar can be jammed. Of course, the targets must have jammers (or at least chaff) and those countermeasures must be used. If we look at the examples of ships that have been damaged or sunk by cruise missiles, we find the following interesting facts. The **HMS Sheffield** ***possessed both chaff dispensers and an electronic support measures (ESM) system [72]. The Sheffield had a weakness in that its satellite communications (SATCOM) interfered with the ESM system. At the time the*** **Sheffield** ***was hit, it was using the SATCOM and had the ESM system turned off. Because of this it did not have enough warning of the attack to dispense chaff.***

Thus, although it possessed systems to protect itself, the* Sheffield *was unable to do so, because those systems were turned off [34], [35]. After the Sheffield was sunk, surviving members of that ship class received radar-jamming equipment at their next overhauls.

The* USS Stark *did not possess a jammer, but it did possess an ESM system, chaff dispensers, and a CIWS system [59]. However, when the Stark was hit, the chaff dispensers were not armed until just before impact and the ship was oriented such that the incoming missiles were in the blind spot of the CIWS (CIWS cannot shoot through the mast and superstructure). A breakdown in the chain of command prevented defensive systems from being employed [36].

The* HMS Glamorgan *possessed ESM, active jammers, and chaff dispensers [72]. It was approximately 18 nmi offshore when a visual streak of light was observed heading for the ship. The ship immediately fired a SeaCat missile, belatedly fired chaff, and turned stern on to the incoming missile [34]. The author has seen no mention made of the ESM system giving any warning or the jammers being activated. It is possible that they were inactive because there was no air threat in the vicinity. The Argentines did not possess any land-launched antiship missiles, so no threat was anticipated from that source. The Exocet that struck the* Glamorgan *was an air-launched version whose launcher had been removed from an aircraft and mounted on the back of a flatbed truck. An inventive enemy is always a threat.

The* Atlantic Conveyor *was a container ship taken up from trade. It possessed no defensive systems. However, it was located in the middle of a multitude of warships, all of which possessed jammers and/or chaff dispensers. All of the warships that detected the incoming missile employed their countermeasures (mostly chaff, but some active jamming) in a timely fashion. Apparently, the missiles locked onto a chaff cloud from the* HMS Ambuscade. *Unfortunately, as one of the missiles emerged from the cloud, it found the only unprotected target (the* Atlantic Conveyor*) in its seeker field of view, locked onto the new target and struck the* Atlantic Conveyor *on the port quarter. The missile penetrated to the vehicle decks and started a fatal internal fire [73]. In summary, no ship that had a certifiably operating radar jamming system or chaff system has ever been hit by an antiship cruise missile.

NPC should develop a comprehensive electronic warfare capability that includes the ability to counter precision-guided weapons. Success in this area will negate another of the critical U. S. advantages and turn that advantage into a liability. The United States has long possessed the systems knowledge to counter its own precision-guided weapons. Jamming of laser-designated weapons has been demonstrated by both expendable jammers and permanently-installed jammers, but the U. S. never deployed such systems. Presumably it did not see a significant threat from any adversary other than the Soviet Union, whose precision guidance capabilities lagged considerably behind America's. Laser-based infrared jammers have been studied for years. However, it is only the recent evolution of image-based infrared anti-aircraft seekers that has brought the technology out of the laboratory and into full-scale development programs. The same jamming technologies can be used against infrared or electro-optical fire control systems.

NPC recognizes the threat from U. S. precision-guided weapons and should face no bar to rapid and effective development and deployment of countermeasures. NPC should concentrate on laser-based electro-optical and infrared countermeasures systems. The systems developed should be capable of negating laser-designated weapons, terminal infrared imaging seekers, and electro-optical fire control sensors. The countermeasure systems should be produced in large quantities and should be deployed on all kinds of platforms at every level. Critical fixed sites (bridges, bunkers, revetments, logistics depots, headquarters, etc.), aircraft, ships, and land vehicles should all receive appropriate protection.

NPC aircraft and naval vessels should also be supplied with state of the art electronic warfare systems including ESM, chaff/flare dispensers, and jammers. Each platform should be equipped with the optimum system for handling the specific threats that platform is expected to encounter. If NPC is not capable of developing the sophisticated ESM and jamming systems, then it should procure them on the international arms market.

The U. S. development community needs to recognize and internalize that viable countermeasures exist or can be developed against every precision-guided weapon currently in the U. S. inventory or in development. The author is continually amazed and distressed at the lack of countermeasures understanding and sophistication possessed by many weapons designers. Their primary reason for being is to make the system work. They are so absorbed in this task that few bother to ask, "How can I make this system fail?" Fewer still are capable of answering the question. These designers are aided and abetted by program managers that do not really want the question answered during their brief tenure on the project. This approach to design and development needs to be replaced by one with a longer-term and more militarily realistic perspective.

The U. S. should strive to develop counter-countermeasure technology applicable to defeat the countermeasures that exist against each of our precision-guided weapons. Those counter-countermeasures should be incorporated into each system where it is deemed cost-effective. Research and development into alternative forms of precision guidance should also be undertaken. That and any other new R & D should consider the certainty of countermeasure techniques and strive to incorporate immunity against as many as possible before initial systems are produced.

CHAPTER 6. ATTACKS ON C^{4}I ASSETS

ATTACK BY ELECTROMAGNETIC WEAPONS

It is difficult and costly to harden weapons systems against nuclear electromagnetic pulse (EMP) [74]. See Appendix A for a technical discussion of EMP**.** ***It is just as costly to maintain and test the special design features that make EMP hardening possible. It is even more difficult to harden weapons against the higher frequencies produced by high-power microwave (HPM) weapons [75], [76].*** See Appendix I for a technical discussion of directed energy weapons (DEW) including HPM**.** ***Without EMP/HPM hardening, our detection, tracking, & navigation sensors can be destroyed, command, control, & communications systems can be knocked out of action, computer systems can be crashed, and even electrical power distribution networks can be damaged. As the threat of nuclear warfare with Russia slowly fades, the willingness of the Department of Defense to fund the EMP hardening of new systems will continue to decrease. Even during the height of the Cold War, funds for EMP hardening of all but the most critical systems were often subject to reprogramming when program costs grew beyond expectations. As emphasis on EMP decreases, it will be harder and harder to justify the extra maintenance burdens necessary to maintain EMP hardness. Any country with even a single nuclear weapon is capable of creating a devastating electromagnetic pulse over an entire theater.***

Even if nuclear weapons are not available, their tactical counterparts (HPM weapons) are receiving increased study by almost every military power. If the United States does not continue to emphasize EMP/HPM hardening and maintenance, and provide the needed level of funding, then our weapons systems will become progressively more vulnerable to EMP. Even a third-rate military power might be able to completely disable key elements of a carrier battle group at a critical point in an engagement. Civilian computer networks are even more susceptible to damage and disruption by HPM weapons, because there has never been an incentive to expend the resources required for hardening.

NPC should make sure that its own electronic systems are adequately hardened against nuclear EMP and against any HPM weapons the United States or its allies are determined to be developing. It should also make sure that the hardening is rigorously maintained and that all personnel are aware of how their actions might compromise EMP/HPM hardness. Full-scale EMP/HPM test facilities should be built to verify the hardness of all critical NPC systems. If NPC is a nuclear power (declared or otherwise), at least a few of its nuclear missiles should be configured for optimum EMP generation and reserved for that mission. To minimize the risks of having the United States escalate to using nuclear weapons, the initial use of an EMP detonation should be localized over the denial area where its effects will only impact the local forces engaged in the conflict and not affect either NPC's or America's strategic systems. Timing of the use of EMP weapons should be early in the engagement, but well after hostilities have been openly declared, to prevent American from claiming that NPC has perpetrated a nuclear "Pearl Harbor". Research should be performed into non-nuclear generation of EMP. This is to be distinguished from research into HPM. The non-nuclear EMP should emphasize high-field strengths over limited areas at the low frequencies that will couple into communication systems and power grids, still considered to be significant targets.

Research and development of high-power microwave (HPM) weapons should also be pursued. Special emphasis should be placed on HPM weapons that can be remotely delivered by ballistic missiles or air-launched guided missiles, or that can be employed as terminal air defense weapons. The former may be targeted at specific U. S. systems, such as air search radars, electronic support measures, or missile tracking radars, or may be intended solely to generally harass U. S. electromagnetic systems. The air defense weapons should be designed to destroy enemy guidance and targeting systems. This will provide additional protection to critical NPC assets should the U. S. be able to conduct a long-range strike with cruise missiles or land-based aviation. Development of battlefield HPM systems should be of lesser importance. Close-in ground combat is usually an indication that access denial has failed. However, short-range (100-200 m) HPM weapons should be developed for special operations force and sabotage use. These weapons may be used to disable critical computer and communication systems in the United States or its allies.

The U. S. has specific criteria for hardening systems against nuclear EMP. However, support and funding for enforcement of these criteria in development programs waned as the probability of full-scale nuclear war decreased as the Cold War ground to an end. However, the threat from electromagnetic weapons will not gradually go away. If anything, it will continue to get worse. The U. S. needs to develop criteria for hardening systems against high-power microwaves (HPM) and non-nuclear EMP weapons. Military procurements should require that these levels of hardness be met <u>at the system level</u>. Procedures need to be developed for assurance that the required hardness levels are maintained over time. Program offices need to ensure that adequate funds are available to support increased hardness in the initial procurements and that assurance programs are funded throughout the life cycle.

Commercial electronic systems are as vulnerable if not more vulnerable to electromagnetic weapons as are military electronics. Because many of these commercial systems are vital to the national defense, the U. S. Government should establish incentives for commercial systems to follow the same hardness and assurance guidelines, especially in critical sectors, such as banking, securities exchange, communications, and transportation.

ATTACK BY HIGH-ENERGY LASERS

Ever since the first laser was demonstrated by Theodore Maiman at Hughes in 1960 [77], the military has found applications for them. Laser rangefinders were fielded in the mid-1960's and laser designators for laser-guided weapons became operational a decade later. Today lasers are used for purposes ranging from precision gyroscopes to wideband communications to gunsights for small arms to countermeasures against enemy sensor systems. Almost from the beginning, far-sighted military researchers recognized their potential as air defense and anti-missile weapons [78]-[81]. See Appendix I for a technical discussion of directed energy weapons (DEW) including optical countermeasures and high-energy lasers (HEL)**.** ***Many programs pushed laser systems to higher and higher powers. Foremost among the programs of the 1970's and 1980's were the Air Force's Airborne Laser Laboratory (ALL) [79] and the Navy's Mid-Infrared Advanced Chemical Laser (MIRACL) [82]. The latter system along with its SEALITE Beam Director pointing and tracking subsystem was transferred to the Army to be part of the national High Energy Laser System Test Facility (HELSTF). Both ALL (using gasdynamic CO_2 laser technology) and MIRACL (using deuterium fluoride chemical laser technology) were successful in that they were able to shoot down tactical missiles in flight. In the same time frame significant developments were being made in adaptive optics [83]. This technology allows atmospheric distortions caused by atmospheric turbulence and thermal blooming to be corrected. This permits tight focusing of the laser radiation on the target.***

A recent follow-on to the ALL is the Airborne Laser (ABL) [84]. The ABL is currently in Program Definition and Risk Reduction (PDRR). Transition to Engineering and Manufacturing Development (E&MD) is planned for 2003 with Production scheduled from 2004 to 2008. The ABL is based on a chemical oxygen-iodine laser (COIL) and is planned as a theater missile defense system. With a nominal 400-km range, it will orbit over friendly territory and destroy short-range missiles during their boost phase. The Tactical High Energy Laser (THEL) is a cooperative venture between the United States and Israel [85]. This small deuterium fluoride chemical laser is to be the prototype of a system designed to destroy small tactical missiles (such as the Katyusha) in flight. Another program still under active development is the Space-Based Laser (SBL) [86]. This hydrogen fluoride chemical laser program has been active since the early 1980's. All of the component technologies of this system have been demonstrated. The next step is a space flight test sometime early in the 21st Century. The SBL is intended to provide a space-based component to National Missile Defense.

The application to ballistic missile defense is the foremost driver of high-energy laser development. Any country with viable HEL systems can provide a measure of such defense to its forces. However, this is not the only important application. The Navy is still interested in HEL systems for cruise missile defense. Their studies have shown that a different laser is required for this application. The Navy is emphasizing free-electron lasers (FEL) [87]. They show the potential for high efficiency, environmental friendliness, and ability to be packaged in a form amenable for incorporation on ships. FELs are still in the development stage, so naval applications are some years away. The high rates of kill (possibly as high as one per second) with virtually unlimited magazine size that might be achieved in advanced HEL systems may be the only viable counter to massive saturation cruise missile attacks against our

battle groups. Line of sight limitations make HELs somewhat less attractive for land-based cruise missile defense, but they should still have considerable effectiveness.

Another possible application of HEL technology is as an antisatellite weapon. A space-based HEL could destroy any satellite that crossed into its "hemisphere" of coverage. Within a few hours it could target almost any other satellite. A ground-based HEL could target any satellite that passed overhead. With proper siting of ground-based site, this would not be much of a problem, as many satellites of military interest must pass over enemy territory to be effective. More details will be found in the section on antisatellite weapons. In a similar vein, HEL technology might prove a viable counter to transatmospheric aircraft. High-energy lasers could also be used as battlefield antisensor weapons or as antipersonnel weapons, although at this point it does not seem cost-effective to use them in this role.

Many countries are pursuing high-energy lasers for a variety of applications. There are a number of commercial applications of lasers in the hundred-kilowatt-class. Although many military applications require megawatt-class lasers, hundred-kilowatt-class lasers could find military use and can often be scaled to megawatt-class devices. Russia, United Kingdom, Germany, France, Japan, and China are among the countries with serious interests in laser technology.

High-energy lasers will be such an important component of warfare in the 21st Century that without a command of the technology NPC can hardly be considered a peer competitor. If it does not already have one NPC should establish a vigorous laser research program. This program should probably be four-fold; that is, it should pursue chemical devices, COIL devices, FELs, and more traditional solid state lasers. It should emphasize that mission that contributes most to NPC's overall strategy. This is quite likely to be the antisatellite mission (because the U. S. is so heavily reliant on satellite technology for much of its warfighting capability). If NPC has a major space launch program, then it should consider space-based HEL systems. If NPC does not possess a strong capability in space (or if it cannot devote more of its budget to this sector because of inter-service rivalry) then it should consider ground-based or airborne HEL systems. Airborne systems would be more difficult to implement, but possess more versatility. A ground-based HEL is useful primarily as an antisatellite weapon. An airborne HEL might be adapted to TBM defense, cruise missile defense, and the battlefield anti-sensor role. An airborne system is also considerably less vulnerable to attack by ballistic missiles, cruise missiles, transatmospheric aircraft, or special operations forces, because it can move from base to base.

The U. S. should be as concerned about an adversary's development of high-energy laser (HEL) technology as an adversary should be concerned about ours. They will revolutionize warfare. The U. S. should continue to investigate countermeasures and other defenses against HELs. Countermeasures will be more effective against some HEL applications than against others.

In the anti-satellite role for HELs, moderately effective countermeasures exist. Solar panels for electric power can be replaced with radioisotope thermal generators that have damage thresholds many –orders of magnitude higher than solar cells.

Damage from general thermal overload can be delayed by incorporation of thermal sinks incorporating phase-change material (the laser energy is channeled into melting a solid rather than heating the entire structure). Enough phase change material could delay overload for minutes, possibly long enough for the satellite to pass beyond range of the HEL. If this occurs, the thermal sink can re-radiate enough of the absorbed energy to return to its initial state. This would permit re-engagement time and again without damage. These and similar countermeasures should be incorporated into new satellites wherever practical.

In other roles for HELs the best defense may be a good offense. If the adversary develops an airborne HEL with 400-km effective range and the U. S. develops one with 500-km range, then the longer-range system should be capable of engaging and destroying the shorter-range system. From this perspective, the U. S. should make every effort to maintain the obvious lead it possesses in HEL technology and applications. Once adequate systems have been fielded, the U. S. should not rest on its laurels; it must strive to field even better systems. Paraphrasing the words of Thomas Watson, former chairman of IBM, "If the U. S. stops trying to be better, it will stop being good!"

ATTACK BY INFORMATION WARFARE

The growing dependence of U.S. forces on network-centric warfare [88] as well as the growing network-dependence of the entire economy and civilian infrastructure of the United States makes us extremely vulnerable to information warfare (IW) [89]-[91]. A detailed discussion of information warfare can be found in Appendix J. ***The efforts of a mere handful of youthful hackers have proven time and again that networks can be penetrated and exploited or damaged. Critical hardware can be crashed. Data and/or programs can be stolen, erased, or even subtly altered (the latter having the capability to produce almost any effect imaginable). Transportation systems, financial networks, communications systems, and utility distribution systems are targets whose large-scale disruption could cause unimagined havoc.***

In the military, there are numerous computer-based systems that are conceivably vulnerable to information warfare. Invaluable intelligence data is stored in electronic databases. War plans may be stored in digital format. Logistics is controlled entirely by computers. Command and control flows over computerized information networks. Self-defense weapon systems cannot function without computers and complex software. Infowarriors might break into classified networks and steal the intelligence data, possibly compromising future intelligence operations. They might be able to covertly copy the war plans and devise strategic counters or ambushes for our forces. The logistics network might be crashed at the worst possible time, hopelessly tangling the system. Alternatively, critical supplies might be routed to the wrong commands. Consider the effect of Navy 5" artillery rounds being delivered to Army units equipped with 155-mm howitzers, and vice versa. The command and control network might be sabotaged in such a fashion that commands might be subtly garbled to result in ill-conceived deployments and inappropriate timing for maneuvers. The self-defense weapons system software might be covertly reprogrammed to intentionally miss only a particular class of antiship missiles emitting a particular signature. None of these effects might become apparent until after the shooting had started.

Information warfare may be the most cost-effective means of attacking the United States. A single, brilliant individual with a personal computer connected to the Internet, who is thoroughly committed to the task, has demonstrated that he can wreak havoc and cause millions of dollars of "damages" **[92], [93]** ***in a few hours time. Imagine the effects that a well, trained Corps of such individuals (properly organized, led, and working in teams of appropriate size) could have.***

The attacks need not be conducted by an organized group. If an adversary has patience, a small number of individuals could infiltrate critical organizations and embed logic bombs or backdoors into critical software months if not years in advance of any attack. This capability is exacerbated by the trend towards purchasing commercial off-the-shelf (COTS) software. The commercial firms seldom obtain high-level government security clearances for their employees. It would be relatively trivial for a handful of programmers with loyalties to an adversary nation (or as suggested in the latest Tom Clancy novel, loyalty to our own government [94]) to be hired by a company like Microsoft, Apple, or Sun Microsystems. It would easy for them to insert logic bombs or backdoors into such ubiquitous programs, such as word

processors, spreadsheets, or even operating systems, in the course of their normal code writing. What if 9 out of 10 personal computers in the U. S. had an unsuspected security flaw that would allow an adversary to gain administrator privileges on any such machine that was connected to the Internet? Are we sure that Windows NT or Linux or MacOS are currently free from such malicious added code?

NPC should strive to achieve technical parity with the United States in the computer, networking, and software arenas. If this is the information age, NPC must be a leader, not a follower. This is true in both the civilian and the military arenas. Computer technology must be introduced into every classroom at every level. The entire NPC society must become computer literate. NPC university students should be encouraged to study computer technology and software engineering at major U. S. universities to learn the latest in U. S. capabilities. Study at universities in other countries leading the information revolution should also be encouraged. After obtaining their degrees, a number of students should be encouraged to work for several years in U. S. information technology companies. Naturally, they will be expected to learn as much proprietary information as possible before their recall to NPC. Furthermore, from time to time they would be expected to cooperate with NPC's information warfare community and covertly plant "strings of code" in the programs upon which they worked. NPC university faculty should be encouraged to take sabbaticals in the United States and elsewhere. They should be encouraged to engage in cooperative research with U. S. companies. Conversely, only a limited amount of U. S. students and faculty should be permitted to study at NPC schools. Very few of these should be permitted to learn anything about NPC corporate technology.

A fraction of NPC's R&D effort will quite naturally be spent on computer and network security including studying the means of attacking computers and networks, in addition to studying the means of preventing such attacks. It is anticipated that this fraction of the program will be conducted under deep secrecy. Computer "hacking" by young people under subtly-controlled conditions should be encouraged. It can serve as a means of developing a cadre of information warfare "soldiers", while channeling youthful energies that might otherwise be turned to "destructive" purposes (such as protesting for human rights). The more adept hackers can serve as useful testers of computer and network security systems being developed. The subtle control alluded to above should include covert automatic monitoring and recording of every keystroke on the hackers' computers. This will provide insight into any new techniques the hackers might discover and will warn authorities if any unauthorized activities, such as sabotaging important NPC systems, are being performed.

NPC must beware of U. S. attempts at using information warfare against it. What NPC plans to do to the U. S., the U. S. may plan to do to NPC. Every software program imported from anywhere should be analyzed for obvious IW features. Mission critical or widely distributed software programs should be reverse-engineered and studied line-by-line by IW analysts to determine what every command actually does. Any unexplainable code should be deleted. Although NPC may abide by copyright and piracy agreements, this does not preclude government configuration control and distribution of sanitized versions of any software product.

The U. S. should continue to devote significant research and development to the field of information warfare and defense against information warfare. There is a critical need to know what can be done to computer systems, how it can be prevented without destroying the usability of the computer systems, and how the systems can be fixed or ameliorated if it cannot be prevented.

Of special concern is the fact that information warfare need not target military systems to have profound effects on military operations. Practitioners should always keep in mind that the military has little or no control over and little or no ability to fix problems in the computer systems present in the civilian sectors of the economy. For this reason, it is not clear that the high levels of secrecy currently afforded to information warfare developments are warranted or even desirable. Consider an information attack on the traffic light system in San Diego that causes a delay in deployment of a carrier battle group because needed personnel and last minute supplies were stuck in monumental traffic jams. Classified knowledge of how to prevent such an attack would be worthless, if that knowledge were not disseminated to the city agency that controls San Diego's traffic lights in time to prevent the attack from occurring.

This example could be multiplied a thousand-fold. Civil sector computers control all aspects of transportation, communication, production and distribution of goods, commerce, and information exchange. This will be exacerbated as the current trend towards government out-sourcing reaches its zenith. Even the military logistics supply line might ultimately be controlled by an overnight delivery service. Information attacks on the computers at the delivery service headquarters might result in the entire inventory of a critical component being shipped to a front organization of the adversary. From there that inventory might be destroyed or transshipped to the adversary after another attack was made on the computer system of U. S. Customs. Everyone needs to know how to protect his system from information attack, because anyone could be the weak link in a complex chain of civilian actions that makes a military operation possible.

Special attention should be paid to the handful of software packages that almost everyone uses. These would include Windows, PowerPoint, Excel, Word, WordPerfect, 1-2-3, and a few others for IBM compatible machines, the operating systems (UNIX, Linux, MacOS, etc.) for other machines, and the major anti-virus programs. The U. S. should investigate these programs on a line-by-line basis to determine their security. Software companies might wish to performed more detailed background investigations on their employees if they wish to sell "certified safe" software to governmental or corporate entities.

ATTACK BY ANTISATELLITE WEAPONS

America depends on its superiority in space (intelligence, surveillance, navigation, and communications satellite networks) to fight efficiently with limited numbers of combatants. The trend to network-centric warfare will continue to exacerbate this dependence. American satellites are not adequately hardened against any form of antisatellite weapon: fragmentation warheads, terminally guided kinetic energy projectiles, or nuclear explosives.

Fragmentation antisatellite (ASAT) weapons place thousands of small fragments in the path of an oncoming satellite. A small explosive charge disperses the fragments in an expanding cloud. The explosive charge can be quite small as the fragments do not need energy from the explosive to provide penetration (as is required in terrestrial fragmentation warheads), the orbital kinetic energy is more than sufficient. The kinetic energy of one or more fragments punches holes in and destroys one or more critical subsystems of the satellite (such as the solar power system, the attitude control system, or the communications link). Such weapons cannot be defended against after the weapon closes to within detonation range. Physical destruction of the attacker at long ranges before intercept is one of only two practical countermeasures. Early warning (minutes) of an impending attack coupled with a substantial orbital maneuvering capability (permitting the target satellite to escape orbital intercept with the attacker) is the other. Since the attacker will likely have at least some form of orbital maneuvering capability (to permit achieving the intercept in the first place), the defending satellite must have an even greater capability. Fragmentation ASAT weapons need not be very large. The mass of fragments required is directly proportional to the square of the accuracy that can be achieved in an intercept. Intercept accuracies of the order of 10 meters might require roughly 10 kg of fragments, while intercept accuracies of 100 meters would require more like 1000 kg of fragments. Fragmentation ASATs can be placed into orbit by any suitable launch vehicle, including large superguns (after they have been developed).

Kinetic kill vehicles (KKV) with terminal seekers (similar to those under development for ballistic missile defense) can also be used in an ASAT role. These may be placed in orbit for employment on command, or they may be launched via direct ascent to impact. On-orbit systems will require a boost motor and orientation system in addition to the kill vehicle. The additional systems are intrinsic to the launch vehicle in the direct ascent systems. Once the attacking system is placed in the right orbit, its seeker acquires the target and a divert thruster system accelerates the kill vehicle (at right angles to the orbital energy) to achieve precision guidance and impact with the target. As with fragmentation antisatellite weapons, the only defenses are running to a different orbit or destroying the kill vehicle before a ballistic intercept trajectory can be established. The former is difficult given the potentially high divert ability (as much as 50-100 km laterally) of a kinetic kill vehicle. Direct ascent ASAT systems can be orbited with relatively modest launch vehicles. The United States demonstrated an ASAT that was launched from under the wing of an F-15. The speed and altitude of the F-15 functioned as the first stage of the launch vehicle. The interceptor was relatively lightweight. There is no reason it should have weighed more than 50 kg. Numerous designs for KKVs weighing between 2 kg and 100 kg were developed during the peak of activity of the Strategic Defense Initiative (SDI). On-orbit ASATs will be larger, probably in the 100+ kg range. Nev-

ertheless, a single medium launch vehicle such as Titan, Delta, or Ariane could put dozens of KKV ASATs in orbit in a single launch.

Nearby nuclear detonations can damage the hardest electronic systems with intense x-radiation, gamma radiation, and neutrons. A 20-kiloton exoatmospheric detonation will illuminate objects with an xray fluence in excess of 1 cal/cm^2 at distances over 10 km, a neutron fluence in excess of 10^{11} n/cm^2 at distances over 11 km, and a gamma ray dose rate in excess of 10^9 rad(Si)/sec at distances over 14 km. Any of these exposures is commonly assumed to be fatal to a typical electronics system. The distance over which these lethal exposures can be produced scales as the square root of the yield, so the lethal range of a 1-megaton detonation is roughly 7 times larger (70-100 km depending on the radiation type). Distant exoatmospheric detonations can produce intense electromagnetic pulses (EMP) over continent-sized areas. This EMP can fry unhardened electrical circuits not just on the ground but in objects passing over the affect region in low and medium earth orbits as well. Furthermore, a nuclear explosion can cause large transient increases in the earth's trapped radiation. This last effect can cause degradation of critical circuits over periods of days to weeks, ultimately resulting in failure, in any satellite passing through the disturbed regions. Even satellites that were on the opposite side of the earth from the detonation are not immune to this last effect. A nuclear ASAT can kill unhardened satellites at extremely large distances. Because of this, there is no need to actually orbit a nuclear ASAT, just get it to the approximate altitude of the satellite target. Since the peak altitudes achieved by ballistic missiles are roughly 25% of their range, a ballistic missile with only 1000-km can place a nuclear ASAT high enough to kill satellites at altitudes as high as 250-300 km. Aiming and timing are not excessively important given the huge lethal radii for exoatmospheric bursts. Even geosynchronous orbit satellites can be attacked with any launch vehicle capable of orbiting such satellites (a nuclear explosive device is much smaller than a typical communications satellite). Satellites can be hardened against nuclear explosives. However, this is extremely expensive and can be defeated by bringing the nuclear weapon closer before detonation. No amount of hardening can protect a satellite system from the detonation of a large nuclear weapon at a distance closer than roughly 1 kilometer.

High-energy laser systems can destroy solar power sources (by melting the solar cell materials and or burning off critical coatings), burn out optical sensors or optical communication systems (by vaporizing detector elements or damaging key optical components), and damage internal electronics (by overheating)[95]. An intensity of 1 W/cm^2 maintained for a period of a minute is almost certainly adequate to damage solar cells or cause serious satellite overheating. The maximum incident solar radiation intensity is only 0.14 W/cm^2. If the laser radiation is in-band to the sensor, then power densities at the detector will almost certainly exceed 1 MW/cm^2. Staring directly at the sun will damage almost any imaging sensor and the specified illumination level is almost one order of magnitude larger than the sun's intensity. A one-megawatt laser can produce 1 W/cm^2 over a 10-m diameter spot. Tracking targets to a small fraction of this spot size has been demonstrated a number of times at ranges of practical interest. Lasers of sufficient power can be easily placed into aircraft or on other satellites (both the Airborne Laser currently in development and the proposed Space-Based Laser are considerably more powerful than the nominal laser considered here). ASAT lasers can also be

placed on the ground. The MIRACL laser already in existence at White Sands Missile Range is also more powerful than the nominal requirement.

Lasers of very modest size and power coupled to small, precision electrooptical pointing and tracking systems can also be to temporarily blind imaging satellites and hide all military activities in the vicinity (10-50 km radius) of the laser. An incident power density of as little as 1 $\mu W/cm^2$ should be adequate to dazzle (using veiling glare) any satellite sensor that is in-band to the laser radiation. A 1-watt (average power) laser operating in the visible or near infrared coupled to a modest 30-cm telescope can produce in excess of 1 $\mu W/cm^2$ over a 10-meter diameter spot at ranges well over 1000 kilometers. Given accurate satellite ephemeris data from some other source and a low-light-level imaging camera at the focus of a second boresighted 30-cm telescope, the system should be able to easily acquire the satellite and track it using the laser light retroreflected from the satellite's sensor. This will work only if the laser is in the sensor's field of view. However, if the sensor is not looking at the geographic region around the laser, then it cannot detect the activity the laser is trying to mask. Such laser blinding systems can be built today without significant R&D investment [95]. They should be small enough to be handled by an individual and carried on small vehicles (such as a HMMWV). They might even be less expensive to produce than the HMMWV.

Although it is relatively easy for an adversary to destroy a number of satellite assets in a very short period of time, it is very difficult for the United States to replace those assets. In peacetime, our satellites have extremely long lifetimes. It is not unusual for a system to have an operational life of many years. This is to be contrasted to Russian satellite systems that had lifetimes of months. Because of the long lifetimes and high cost of our satellites, we do not have an inventory of replacements. The United States neither had to place multiple replacement satellites in parking orbits (to provide ready replacements when one satellite failed) nor to develop a rapid launch cycle time (to permit many launches in a relatively short period of time to accommodate frequent replacement of failed satellites). We also do not have an inventory of satellite launch vehicles. It typically takes many months to build a launch vehicle and many months to several years to build a satellite. It typically takes many weeks to mate a satellite to its launch vehicle and launch that satellite. The lack of a rapid satellite replacement capability coupled with our dependence on our satellite assets creates a serious vulnerability that we should not ignore.

If America's space assets were destroyed, we would be unable to conduct effective military operations. Our cruise missiles and many other precision-guided weapons would be unable to hit their targets because they rely on guidance information derived from GPS satellite signals. Surface ships, aircraft, and even infantry forces would lose the precision navigation capability they derive from GPS. Falling back on residual celestial navigation, inertial navigation, or even map-reading capabilities (if they are still available) would mean going back to living with position uncertainties of kilometers rather than meters.

Theater and higher level commanders rely on imaging intelligence from satellites to provide early warning of troop buildups or maneuvers). Without such intelligence, we are open to tactical and strategic surprise. The same intelligence is used to develop targeting in-

formation for air and missile strikes and artillery fires. Even if the guidance of those weapons were not degraded by absence of GPS, the lack of high-quality targeting information reduces their utilization to Vietnam era quality and results.

Our command and control system relies on wide bandwidth data communication. Loss of communication satellites means that only line of sight communications, line of sight communications relayed by airborne assets, or low bandwidth HF communications will remain. Unit commanders will be reduced to communicating only with direct superior and subordinate commands. Calls for assistance from or coordination with other units will require tedious and time consuming routing up and down multiple levels of command. Even the quality of life benefits of modern technology will disappear. Contact with families over the Internet will disappear for deployed forces. Even telephone communications with land forces will be degraded. Television broadcasts may be terminated if the retransmission satellites are knocked out. Loss of satellite-based Internet service will also cut off deployed administrators from remote databases, maintenance technicians from factory support personnel, and health care workers from telemedicine support.

Commanders will even lack short-term weather forecasts. Images of storm systems will be unavailable. Thus ships at sea will have limited knowledge of the existence or courses of major storms. Commanders will be unable to determine in advance when conditions will be favorable to aircraft operations and when they will no. Essentially, they will be reduced to forecasting the weather based on the appearance of the sky and whether the barometer is rising or falling.

An extended campaign against space assets might even knock out our missile launch warning satellites. Without these satellites the U. S. would be vulnerable to a surprise attack by nuclear ICBMs and SLBMs. We would furthermore lack any immediate indication of the use of theater ballistic missiles. Although we have often rhetorically stated that such attacks on the warning satellites would trigger nuclear retaliation, it is unclear whether we would actually carry out such threats. Against a fully nuclear capable adversary, the threat of mutual assured destruction still exists and without a demonstrated nuclear attack, it is doubtful if our government would trigger a mutually destructive nuclear exchange. If the adversary were not a nuclear power, then our own formally declared policy is that the U. S. will not use nuclear weapons against any non-nuclear State Party to the nuclear Non-Proliferation Treaty that has abided by that treaty. Should a non-nuclear power disable our early warning satellites, it is doubtful that the U. S. would retaliate with nuclear weapons.

In short, in the face of a dedicated attack on U. S. and allied space assets, U. S. forces would be knocked back to Vietnam era fighting capabilities. Our forces would be no better than the forces available to any third world country. Maneuver warfare would once again be replaced with attrition warfare with its high death tolls and emphasis on numerical superiority without force multipliers. It would take years to replace any significant loss in our space assets. Almost any conflict that involved ASATs would be over before we could recover.

NPC should develop extensive ground-based laser and space-based laser antisatellite weapon capabilities with the goal of being able to destroy even geosynchronous satellites. As a backup, it should develop more conventional fragmentation or kinetic energy impact antisatellite weapons. A coherent and cautious strategy should be developed for employing these weapons. If the U. S. believes NPC to possess enough ICBMs to give NPC a mutual assured destruction capability, then destruction of U. S. space assets might trigger a massive nuclear retaliation. This was stated as a likely response to Soviet destruction of our space assets had it occurred during the Cold War. On the other hand, it is doubtful that the U. S. would have actually launched a first strike (and thereby initiated mutual assured destruction) merely because our satellites were attacked, even if it were the ballistic missile launch early warning satellites. Rhetoric is one thing, suicidal action is another. If the U. S. does not believe the NPC ICBM threat to be overwhelming, then U. S. space assets could be attacked with very little fear of instant massive nuclear retaliation.

If space attack is not ruled out, then antisatellite assets should be employed in a manner to deny the U. S. specific targeting information at the most critical moments. That is, the attacks on U. S. imaging satellites should be timed to occur at the precise moments that U. S. forces entire the denial area. Premature employment gives the U. S. a capability to launch limited replacements for its destroyed satellites. As it will likely take at least a week for a satellite to be mated to a launch vehicle and readied for launch even under emergency conditions, optimum attack timing can have a profound impact on U. S. warfighting capabilities. Given the U. S. reliance on GPS, it is clear that at least half of the GPS satellites should be destroyed. Other space assets such as communication satellites or weather satellites should also be considered as potential targets. A detailed plan for space warfare should be developed. This would establish the space targets to be attacked, the priority placed on each target, the prerequisites for initiating an attack on each target, and the sequence and timing of probable attacks. This plan would also provide guidance for the development of the attack forces. For example, how many laser ASATs versus how many missile ASATs are needed and where should they be deployed.

The use of nondestructive laser blinding systems can deny tactical imaging information without much chance of triggering a nuclear response. Radar and ELINT satellites would be unaffected by laser blinders, so intelligence denial is not complete. NPC should consider building and deploying enough laser satellite blinders to cover all ground and naval forces. NPC should also consider developing laser antisensor capability for use against unmanned aerial vehicles (UAVs), as these will form the major form of in-theater reconnaissance employed by the United States. A laser antisensor weapon would combine a highly-sensitive target acquisition system (most probably based on infrared search sensors and/or laser radars) for detecting the presumably stealthy, high altitude UAVs and a medium-power laser for damaging the UAV sensor systems. Such devices could be evolved from the satellite blinders. A high-power microwave system might also be included to destroy any electronic intelligence or synthetic aperture radars that the UAVs might carry.

The U. S. will undoubtedly develop its own antisatellite weapons. To the extent that NPC relies on its own space assets, it must develop capabilities to protect the functions provided by those assets. NPC should invest in an inventory of spare satellites and launch vehicles. Some of these may be placed in parking orbits and kept inactive. Others should be kept in a ready condition for rapid launch. NPC should attempt to develop automation technologies that would minimize the time required to prepare and launch each satellite. NPC should study protection technologies for on-board systems. It might consider using radioisotope thermal generators for power rather than fragile solar cell systems. It should incorporate nonlinear optical limiting filters in its imaging systems. It should devote a significant fraction of the weight budget to thermal control of satellite systems. These will prevent medium-power antisatellite lasers from having significant effects and may reduce vulnerability to other antisatellite technologies.

The U. S. cannot afford to lose a significant fraction of its space assets. However, this is what will almost certainly happen if an adversary develops a viable anti-satellite capability. The U. S. needs to evaluate what technologies might prove effective as countermeasures to an anti-satellite weapon.

We should incorporate known protection technologies for on-board systems and study new protection technologies. We might consider using radioisotope thermal generators for power rather than fragile solar cell systems. This will provide a significant improvement in survivability against any ASAT technology. We should incorporate nonlinear optical limiting filters in our imaging systems. We should devote a significant fraction of the weight budget to thermal control of satellite systems. These will prevent medium-power antisatellite lasers from having significant effects. The outer surfaces of satellites should be coated with lightweight xray shielding and radiation protection circuits should be incorporated. These latter devices sense excessive radiation levels, store the current state of electronic systems in hardened memories and instant shut off power to the system. As soon as the radiation level subsides, the circuit initiates a restart using the stored information as a starting point. Function is temporarily halted, but neither function nor data are lost. In addition, the entire package should be analyzed and hardened against both EMP and high-power microwaves. These will provide improved protection against nuclear ASATs. Many such measures were planned for implementation in current generations of satellites. It is unfortunate that in the 1990's a fit of post-Cold War budget cutting forced their elimination on the grounds that they were unnecessary. All critical satellites should be provided with larger orbital maneuvering capabilities than their normal missions require. This will permit the satellite to actively evade some of the ASAT threats. It may be worth coupling a collision detection radar system that can track all objects within a nominal range (100 km?) and automatically trigger the maneuvering system if an object appears on a collision trajectory. This would negate the possibility that the adversary might be able to interfere with control from an earth station during the critical moments before intercept.

As a complement to, or at least an alternative to hardening, the U. S. should consider redundancy by placing systems with comparable capabilities into grossly different orbits. Reconnaissance satellites using low earth orbits could be backstopped by a few larger satellites in medium earth orbits. Geosynchronous satellites could be backstopped by a larger number of smaller satellites in Molniya orbits. Such redundancy would force an adversary to develop multiple kinds of anti-satellite weapons in order to ensure that any specific U. S. capability could be eliminated.

Another option is reconstitution of satellite losses. This is a costly option that requires multiple spare satellites held in storage and a substantial number of launch vehicles kept in ready reserve. When a critical space asset is destroyed, a replacement is removed from inventory, placed on a waiting launch vehicle, and launched as quickly as orbital timing permits. This option could be made somewhat less costly by designing cheaper satellites that have very short expected lifetimes. Knowing that they would have to be replaced in three months regardless, there are always multiple satellites and launch vehicles in the production line, with at least one being readied for launch. Although they did not do this intentionally, this was the path the Soviet Union pursued with its intelligence satellites. Had the U. S. expended an anti-satellite weapon to shoot down a Soviet satellite, the advantage would have been much shorter-lived than if the Soviets had downed a U. S. satellite. Because we design our satellites to have lifetimes of years, there is seldom a spare available. When a launch fails, we must sometimes contract for a whole new satellite to be constructed from scratch, and wait months for it to be completed and readied.

Another option is to backstop certain space assets with unmanned, high altitude and endurance (HAE) aerial platforms. For example, in-theater non-line-of-sight communications could be relayed by several HAE vehicles. These vehicles would never have to come into range of the anti-satellite systems (whether ground-based missile launchers or ground-based laser systems). Aerial reconnaissance satellites could be backstopped by planned HAE reconnaissance platforms. In-theater weather measurements could also be performed by several HAE platforms if the U. S. weather satellites were destroyed.

A last alternative is the development of anti-ASAT weapons. The same boost phase defenses envisioned during the heyday of SDI: Space-Based Laser (SBL) or Brilliant Pebbles (BP) can defend against ASAT launches just as they can defend against ICBM launches. In addition, both types of devices should have reasonable effectiveness on weapons that have already achieved orbital velocity and pass within relatively short distances. Having a terminally guided, maneuvering, kinetic kill vehicle, a BP system should be capable of killing ASATS, post-boost vehicles, and even adversary satellites. Although SBL would not be capable of killing an ASAT after boost at it maximum ranges, if the ASAT passed close enough to the SBL it could nevertheless be damaged or destroyed. An SBL would also be capable of destroying adversary satellites.

RELIANCE ON LONG-RANGE AIRBORNE SURVEILLANCE

The United States requires long-range airborne surveillance assets to detect incoming aircraft and missile threats and to keep track of the ground battle. Satellite-based sensors cannot adequately perform these functions. Without AWACS (Air Force) and E-2C early warning and tracking aircraft [96], [97], the airborne forces would not be able to conserve their strength, and use maneuver warfare to gain superiority in only those regions where superiority is required. Aircraft would be required to remain airborne on continuous air patrol in order to intercept incoming raids. The continuous stress on the systems (machine and humans) would soon lead to total breakdown of effectiveness. The J-STARS ground surveillance aircraft allow all vehicular traffic to be monitored in an entire theater of operations [96]. This knowledge allows U. S. forces to prevent the enemy from effectively employing maneuver warfare against the U. S. Without J-STARS United States forces are vulnerable to surprise attack and/or tactical deception. Despite their importance, the United States has a limited number of these airborne assets. The on-board sensor suites are enormously expensive, so the U. S. is not been able to procure as many of these specialized aircraft as some would like. An aircraft carrier has only enough E-2C aircraft to keep one aircraft airborne and fully operational at all times (given standard equipment failure rates). This is due both to cost and to lack of deck space to accommodate too many spare aircraft. Theaters are also severely limited in the number of AWACS and J-STARS aircraft available to the commander. Here too the allocation is typically just enough to keep one (or two, if the theater is geographically large) aircraft of each type in the air at all times. Heroic maintenance efforts might permit the number of available aircraft to be temporarily increased, but this cannot be supported for long campaigns. In general, there is not a large pool of reserve aircraft back in the United States to draw upon if losses become heavy.

Typically, the long-range surveillance aircraft are unarmed (with the exception of electronic warfare assets) and are kept as far away from the enemy as consistent with performing their missions. There are often two or more fighter aircraft assigned to provide cover for each surveillance aircraft, although the covering aircraft may not be dedicated escorts. There may also be an Airborne Laser aircraft assigned to provide missile defense to the surveillance assets. Despite these precautions, the surveillance aircraft can be attacked and shot down. Suppose that the enemy concentrated its "air superiority" efforts early in a campaign on destroying or damaging as many of the long-range surveillance assets as possible. Concerted attacks by large fleets of aircraft might be successful especially if the attack were disguised to look like an attack on other obvious high-value targets. Attacks by ballistic missiles with anti-air submunitions might also prove successful. If the attacks were only marginally successful and downed only one AWACS or E-2C aircraft, then after enough time has passed, it will be likely that airborne surveillance will be missing for at least some part of each day. If two or more were downed, loss of continuous coverage would be almost immediate and substantial. If a J-STARS aircraft were downed then control of the ground war would revert to Korean War vintage techniques (radio links connecting reconnaissance patrols with a coordinating headquarters). In any case the United States would be severely hampered for the remainder of the campaign.

NPC should devote a fraction of its air force budget to systems capable of negating U.S. long-range surveillance aircraft. Long-range (>200 km range), high-speed (>Mach 5) air-to-air missiles with advanced dual mode (RF/IR) countermeasure-resistant guidance should be developed specifically to target high-value air targets. Several teams from each air group should be dedicated to this critical mission. They should develop tactics that will permit maximum surprise and minimum reaction time in the attack. These aviators should be given first rate aircraft to optimize their chances of success. Thought should be given to developing surface-to-air missiles with capabilities comparable to the air-to-air missile, and employing them in a coordinated attack. Long-range ballistic missiles with anti-air submunitions might also be used. If properly thought through, the tactics and weapons used in this attack might also be able to attack the U.S. Air Force's Airborne Laser aircraft (denying the U.S. a critical facet of its short- and medium-range ballistic missile defense capabilities). At the outset of any open hostilities, NPC should be prepared to immediately implement the counter-surveillance strike. NPC forces should strike these assets early and decisively, because as long as those assets are in place, they are major force multipliers for U.S. forces. Once destroyed, it will take the U. S. years to replace those assets.

The U. S. needs to recognize that its long-range surveillance assets are not only vulnerable to attack by a creative and determined adversary, but also very attractive targets to such an adversary. Better protection needs to be afforded to these assets. Consideration should be given to adding improved self-protection equipment – state-of-the-art, dc-to-light, electronic warning, jamming, and decoy systems – to those platforms that do not already have them or comparable capabilities. Consideration should also be given to providing each of these assets with dedicated fighter escort. Finding new tasks for already overtasked forces is not pleasant to contemplate. Comparable levels of protection should be given to our limited aerial refueling assets. Loss of enough tankers will cause the surveillance platforms to land in order to refuel. This will significantly reduce the availability of these assets to such a degree that an additional aircraft may be required. Assigning two or four fighters to escort every AWACS, JSTARS, E-2, KC-10 tanker, etc. will mean that other vital tasks cannot be performed. On the one hand, it makes no sense to have targets, if you have no aircraft to attack them. On the other hand, it makes equally little sense to have aircraft, if you cannot provide them with targets to attack. However, it must be remembered that the roughly $500 million replacement cost for a new 767-based AWACS or a JSTARS could procure a dozen F-15s or two dozen F-16s, and the loss of these surveillance assets could be catastrophic to our new "network-centric" concepts of warfighting. The calculations should be refigured with this new vulnerability (and an assessment of its likelihood of exploitation) firmly in mind. The same kind of analysis of alternatives should be repeated for any of the instances (in the following sections of this report) where escorts of one kind or another are suggested as fixes to the vulnerability.

SUSCEPTIBILITY TO STRATEGIC DECEPTION

U. S. intelligence efforts are dominated by satellite-based systems for imagery and electromagnetic signal interception. Satellite-based intelligence (Satint) is exceedingly susceptible to negation by moving the activities underground. Witness the success of the North Koreans in hiding the exact extent and nature of their nuclear programs. Virtually any activity of any size can be hidden underground, if it is sufficiently important to warrant the expenditure of resources. Submarine bases, factories, infantry barracks, small cities, and even airfields can be constructed underground. Corregidor, Gibraltar, and Cheyenne Mountain among many others are examples of massive military facilities that were located almost entirely underground, although the underground basing was selected for physical protection not secrecy. Satint is also notoriously dependent on the availability of satellite coverage of any region of interest. Frequent observation of one region precludes observation of many others. Over time, continuous observation of underground facilities can yield limited information. However, this is at the expense of failing to observe many other facilities. The U. S. intelligence community has limited human intelligence capability. Humint is the only form of intelligence capable of penetrating buried facilities to uncover secret programs with reasonable expenditure of effort and resources.

The common reclama against hiding facilities underground is that secret weapons developments cannot be employed without extensive training and this training must be carried out in the open. This is the territory of strategic deception [98]. It wasn't possible to hide the massing of several million men and equipment in England prior to the Normandy invasion; it <u>was</u> possible to deceive the Germans as to where and when the invasion would occur [99]. The United States hid the deployment of the Corona spy satellites under the guise of Discoverer scientific missions [100]. Laser weapons tests were routinely conducted when there would be no known foreign spy satellites overhead. The same was true of the ground phases of every stealth aircraft program. Takeoffs and landings were timed to occur at night and when satellite coverage was non-existent. At all other times the airplanes were either hidden by the enormity of the airspace of the western U. S. or hidden by hangars. The windows of opportunity ranged from many minutes to many hours. Plausible alternative activities conducted in parallel with the actual secret activities coupled with disinformation (believable cover stories) can lead any observers to miss the secret activity or ascribe any of its detected characteristics to the plausible alternative.

Large unit training can be disguised by consecutive training of smaller units and disguising the exchange of units between training cycles. Training for one form of warfare may be disguised as training for another form. For example, amphibious operations training (assumed to be provocative and suggestive of offensive intent) can be disguised as river-crossing operations training (which are essential for even a defensive Army). Special operations training (clearly offensive) might be disguised as counter-terrorism training (necessary for any country in today's terrorist-filled world). Prior to March 1935, when the ban on German rearmament was still officially in effect, the German "Air Force" maintained a cadre of basic flight-qualified personnel through a proliferation of soaring clubs – soaring was a German national sport in the '20's and '30's. It subsequently converted the most-promising young

glider pilots into fully qualified pilots through the German Air Line Pilots School (which not too surprisingly was run more like a military academy than a pilot training school). Graduates of this school nominally worked for Lufthansa but many were sworn into the "Black Luftwaffe" as officers and trained to fly fighter aircraft [101]. This subterfuge was known to Allied intelligence organizations because the Nazi leadership could not help boasting about how many advances the Third Reich was making, but it served admirably to support the fiction of "Peace in our time" favored by pacifist politicians such as Chamberlain.

NPC should conceal all of the more provocative aspects of its military buildup under some form of deception or camouflage. When possible, development facilities should be constructed underground. Wherever practical, operational military bases (or their critical parts) should be located underground. Submarine bases should excavated into cliff faces with underwater ingress and egress. Aircraft test facilities should follow the Groom Lake model [102]. Operational airfields should always store aircraft in hardened, covered revetments or in caves or tunnels in nearby hills (so as to make counting the number of deployed aircraft difficult). If covered structures are used, but some are used only as decoys to confuse counting, activities (heating, air conditioning, communications, power usage, etc.) at the decoys should those of the non-decoy (in use) structures. Tunnels complexes that might or might not be used to house military equipment (such as artillery batteries or missile launchers) should be built throughout the country. Those complexes not actually used should be maintained as if they will be used in the near future. In strategic deception, the devil is in the details.

Provocative training exercises should be structured so they look like less-provocative training exercises. Specialized training should be done in small groups on a continuous basis rather than large groups on a one-time basis. Embedded training, virtual reality, and netted training should be emphasized. When entire divisions can simultaneous exercise in interconnected simulators, all aspects of command, control, and coordination can be rehearsed without any outside knowledge of large-scale exercises taking place. When essential to exercise in the open, cover stories should be developed (beginning years in advance). If NPC intends to invade a neighboring country and a large force buildup is required near the border, then such large buildups should be conducted on a regular basis for at least 5 years prior to the actual invasion.

The U. S. needs to address its failures in obtaining adequate human intelligence, that leave us susceptible to strategic deception on a grand scale. The intelligence communities should spend less effort on creating "national technical means" and spend more effort on gathering human intelligence and more effort in analyzing the intelligence (technical and human) that it does gather. Resources should be reallocated on the basis of potential likelihood of conflict and low degree of "presence" in a region, rather than on "the number of nuclear weapons the country possessed", that appears to be the dominant Cold War criterion. Human intelligence efforts should be expended inversely with the degree of transparency the adversary government exhibits. In analyzing technical intelligence, analysts should be trained to consider the potential of strategic deception and concealment on the part of the adversary. Lastly, the various intelligence agencies need to better coordinate their efforts. Each organization has its own "rice bowl" and has little desire to share intelli-

gence and analysis that make help another organization to increase the size of the other organization's rice bowl.

EXCESSIVE INTELLIGENCE-RESPONSE LATENCY

High-value targeting relies on the flow of information from intelligence assets such as National Technical Means through the collection agencies to field commanders to the local units that conduct the actual attacks. Historically, it has taken inordinately long times for intelligence information on critical targets to flow down to the organizations that needed it. It might take hours or days for photo-interpreters to locate and identify a specific target of interest. It might take even longer before that information was transmitted to decision-makers and planners. Even after the information was incorporated into a targeting plan, it takes an extended period of time for an individual weapon to be brought to bear against that target. As a result of the inability of Coalition forces to destroy Iraq's Scud missile launchers, many new initiatives were launched. The whole concept of Network-Centric Warfare is aimed at reducing time delays between acquiring target data and delivering weapons on that target. Unfortunately, no matter how well these concepts are implemented, until speed-of-light weapons are used to perform the actual engagement, there will always remain latency periods of at least a few and possibly many minutes between detection and destruction. This inherent latency can and often is exploited by our enemies.

NPC should make as many of its high-value targets as mobile as is practical. ICBMs and most shorter-range missiles should be mounted on mobile launchers (either truck- or rail-based). Careful design consideration should be paid to minimizing the time a launcher must be stationary to prepare for launch, launch a missile, and pack up for relocation. A maximum of ten minutes is desirable. If possible, designs should allow shoot on the move. Launcher designs should allow them to be camouflaged to look like any of a large number of civilian targets, (e.g., like gasoline trucks, milk tankers, refrigerated semi-trailers, or freight cars), so that while in motion they cannot be readily identified. Similar considerations should be given to artillery and air defense weapons. Given the ability of counter-battery fire to have return fire in the air before the initial rounds have impacted suggests that future artillery should be designed to fire on the move. Fixed site surface-to-air missile unites will be quickly identified and destroyed in the opening moments of a high-intensity conflict. NPC should design all of its air defense weapons to be both highly mobile and to be able to shoot on the move. Fixed site systems such as ground-based lasers that cannot be made mobile should be designed so that most of the target is deeply buried and protected. Redundancy in the critical beam direction components as well as improvisation of special protection mechanisms should be employed to permit those sites to be survivable even after initial targeting.

At the same time NPC should devote considerable effort to the study of the United States' Network-Centric system. It should develop a detailed process model that will allow NPC planners to understand the latency between the creation of a piece of information and its end use. These planners should determine the critical network nodes, whose loss would further exacerbate latency problems. Special weapons or special means of attacking these network nodes should be developed. At any point in the conflict where it appears that the U. S. is operating inside NPC's decision loop, NPC should act to slow the cycle down and should attack those critical nodes.

Intelligence-response latency is best addressed by eliminating as much as possible at the source. Some latency could be reduced almost to zero by directly relaying the satellite imagery to the user. When any competent physicist from any country in the world can unquestionably calculate to within 25% accuracy what the performance capabilities of a given satellite are (without resorting to any information that is not available in the open literature), there is little rationale for continuing to place codeword restrictions on access to raw satellite images. Missile launch indications should not take more than a few seconds to be forwarded to ballistic missile defense units. Intelligence community sensitivities should be overridden in these areas in order to facilitate the rapid sensor-to-shooter communication envisioned by network-centric warfare. Latency at the shooter end can be reduced either by developing weapons with faster times of flight (hypersonic cruise missiles versus subsonic cruise missiles) or by deploying the shooters closer to the target. There are advantages and disadvantages to both approaches. Thus, both should be investigated and pursued where it can be shown to be more advantageous. Latency in the middle (the decision process) can be minimized by a priori *delegating firing authority down to the lowest level. The U. S. military prides itself on the initiative exhibited at all levels of the chain of command. This is one area where <u>pride in the fact not just the promise</u> is not only desirable but also essential.*

CHAPTER 7. UNCONVENTIONAL METHODS OF ATTACK

ATTACK BY SPECIAL OPERATIONS FORCES

All aspects of the United States military and civilian sectors are vulnerable to enemy special operations forces (SOF). This vulnerability results from several factors. Few senior U. S. military leaders appreciate the impact that special operations closely coordinated with conventional operations can have on the outcome of a campaign. For example, during the Persian Gulf war, Gen. Schwarzkopf only grudgingly permitted limited participation by American special operations forces [103]. Conventional American forces seldom train to defend against SOF attacks. Remember the dictum "Train like you fight! Fight like you train!" Furthermore, U. S. forces in rear areas typically exhibit a complacency that invites attack by SOF ("that can't happen here"). This is borne out by the repeated havoc that a single platoon of SEALs was able to inflict on military base after military base during Red Cell security inspections [104]. It is reinforced by the general public perception that "it can't happen here". Remember that the continental United States has not been attacked by a foreign power since the War of 1812 (if you discount Pancho Villa's "banditry" on the Mexican border [105] and the half-hearted Japanese submarine-based artillery shelling of oil storage tanks near Santa Barbara [106] and "fire-bomb balloon" attacks on the Pacific Northwest [107] during WW II).

Although the public is aware of and somewhat enamored of the almost unbelievable capabilities possessed by U. S. Army Special Forces and Navy SEALs, few members of that public know that highly capable special operations units are possessed by almost every major military power. They cannot bring themselves to imagine that comparable capabilities might be directed against themselves by a foreign power. Consequently, they are not adequately prepared (physically or mentally) to deal with attacks by special operations forces. However, with relatively little investment any peer competitor could possess special operations forces that are almost the mirror image of those of the United States (although the U.S. might retain a slight edge in high tech gadgetry for equipping those forces). Any mission that the U. S. has envisioned to be performed by our own special operations forces could just as easily be performed against us by enemy special operations forces. Sabotage, assassination of key political or military figures, neutralization or destruction of critical facilities, intelligence gathering, deep reconnaissance, capture of ships, offshore platforms, or other critical facilities, or diversionary raids can be directed against us just as we have envisioned using them against our own enemies.

There is the additional possibility that terrorists (both foreign and domestic) might be enlisted to conduct attacks against U. S. assets at home or abroad. This would not entail any significant effort or cost on the part of an adversary. Nevertheless, perhaps the only things that would distinguish terrorist attacks from special operations forces attacks are the professionalism and consideration for limiting collateral damage that special operations forces would exhibit. All U. S. forces have proven themselves vulnerable to terrorist attack time and

again. The bombing of the Marine Barracks in Beirut, the bombings of nightclubs in Germany frequented by U. S. soldiers, the bombing of the Khobar Towers apartments, and the bombing of the U. S. S. Cole.

This last incident points out a serious SOF/terrorist threat to U. S. naval forces. Many navies are moving away from large blue-water ships like destroyers and cruisers towards patrol boats and even modified pleasure craft. A boat the size of a large cabin cruiser (such a WWII PT boat) can carry several antiship missiles or 2-4 torpedoes and one or more guns as large as 40-mm. The addition of several handheld missiles (such as Stingers) can provide a credible air defense. Any of these craft is capable of sinking a destroyer or a cruiser. Furthermore, several dozen might be acquired and armed for the cost of acquiring a single Aegis cruiser or destroyer. Fighting several dozen missile- and torpedo-armed patrol boats is considerably more difficult than fighting a few destroyers.

Even smaller boats can be equipped with crew-served anti-armor weapons. A TOW missile launcher (chosen because at least 36 countries currently have this weapon – the French, Swedish, Russian, or other equivalents are equally serious threats) can be mounted on craft as small as an inflatable boat such as a Zodiac. One could easily be mounted and concealed on any small fishing boat, coastal trader, or pleasure boat. Nevertheless, the missile could be launched at ranges up to 4000 meters and precision-guided to seriously damage any warship. The warhead of a TOW missile could: destroy the bridge of a destroyer, damage half the faces of a SPY-1 radar, completely destroy any other radar or electro-optical sensor system, put a large caliber gun out of commission, damage the steering mechanism of many ships, or incapacitate an aircraft elevator on an aircraft carrier. In ten seconds an innocent fishing boat could transform itself into a gunboat and fire a small missile at a passing warship. Any boat even a dinghy can carry enough high explosive to blow a large hole in the side of any warship. In littoral waters it is difficult to avoid having small boats come too close for safety. Many Asian fishing boat captains play "tag" with larger ships. It is considered good luck if one can successfully cut across the bow of a larger vessel. The act reputedly stops demons from following the smaller boat. Such acts could only be prevented by firing on the boats (and except in wartime this would not be permitted under international law). Sooner or later, one of the crews of these boats will be consist of terrorists or special operations forces, and one or more warships will be damaged, and possibly put out of action.

NPC should expend every effort to create a substantial & credible special operations force with global reach. These forces should be capable of performing a full spectrum of special operations. They should include components capable of sea, air, and land operations. The SOF should be equipped and trained to be the equals of U. S. Special Forces or SEALs. The NPC military leaders should develop a doctrine that recognizes the importance and advantages of SOF while also appreciating their limitations. That doctrine should permit the use of SOF with conventional forces in a fully coordinated fashion whenever possible, while retaining the option and capability for independent SOF operations.

Creation of a first-rate special operations force cannot be accomplished in a few days or even a few years. However, if NPC is willing to devote adequate resources and the better part of a decade to the attempt, then the path to success is straightforward. It requires continuing and unrelenting emphasis on mental and physical conditioning, teamwork and unit cohesion, and realistic mission training. The following hypothetical course of action is only suggestive of how NPC might develop its special operations forces.

NPC might begin by assembling a moderate but manageable number (approx. 100) of volunteer career officers and senior enlisted personnel. This unit should undergo extensive physical and psychological toughening under the direction of experienced former special operations personnel. There is no shortage of retired Special Forces, SEALS, SAS, GSG-9, Spetsnaz, etc., personnel who could be hired to provide the initial training required. An extended severe mental and physical test (such as Hell week, the "crucible", etc.) is important to both the selection process and to team building. After the first few months of conditioning, basic special operations skills (shooting, unarmed combat, silent movement, etc.) may be added to the training regime. After six months to a year of this training to weed out those without the physical and mental stamina for special operations, the NPC personnel should become part of the training cadre. Additional forces may then be sent through the training regime. After several training classes have been graduated, the first advanced training units may be established. Such units should be small (8 to 14 enlisted with 1 to 2 officers) with officers that are treated little differently from enlisted. The total organization should be horizontal with a minimum of military formality and hierarchy. Unit personnel should only be shuffled if required due to casualties or dropouts. After an extended period of advanced training it is envisioned that these units would become operational.

The advanced training units should continue training under the outside special operations experts. Weapons, tactics, demolitions, close quarters battle, parachute training, and underwater operations are logically part of the training schedule at this level. Unit training must be as realistic and as intensive as possible. NPC must not balk at providing its SOF units with all of the weapons and ammunition that they can possibly use. After a minimum of six months at the unit level, the unit may be considered for conversion to operational status.

Operational units should continue advanced training on their own. Oversight by foreign mercenaries should not be necessary nor desirable at this stage. For the first few years, operational units should be given operational missions sparingly. Each mission needs to be carefully considered beforehand based on the degree of secrecy planned for the operational forces as a whole. It is also relatively important to have more early successes than failures. Special weapons & equipment and extensive rehearsal must be provided for any operation mission. It is during this period of initial operations that an overall strategy of SOF employment can be developed and evaluated. After two to three years on operational status, individuals in the unit should be rotated back into the training cadres and into newly formed units to facilitate the spread of operational knowledge throughout the force. If the training input is large enough to guarantee more "graduates" than the force loses through attrition, then the number of operational units will steadily increase. No sooner than four or five years into the process, a "publicly acknowledged" force might consider attempting cross training with SOF forces of other countries to provide independent evaluation of the acquired skills. Over time, the more highly skilled members of the earliest classes can replace the mercenary training cadre. After a decade or so, a large well-trained and self-sustaining force will have been created. Attaining proficiency comparable to U.S. special operations forces will require many years of continual training in all operational skills and dedicated support on the part of the rest of the military forces.

If the existence of these forces is not intentionally kept secret (a difficult but possibly very desirable undertaking) then those forces should actively cross train with U. S. special operations forces. This would help to guarantee maximum readiness, access to the latest techniques, technology, and equipment, and better preparation to counter the U. S. forces when conflict comes. To facilitate U. S. willingness to permit cross training, all externally visible training and preparation should emphasize "acceptable" and "peaceful" roles such as counter-terrorism, hostage rescue, anti-piracy, or drug interdiction, rather than uniquely military operations. Training for the uniquely military missions should be done in a fashion that gives the U. S. minimum information on those missions and SOF's ultimate capabilities.

At the onset of hostilities NPC should employ its SOF (in concert with any other intelligence or fifth column assets in place) to disrupt the U. S. military machine and its preparations to the maximum extent possible. Using conventional or special weapons (as NPC's policy permits), they should attempt to disrupt embarkation of troops and materiel at critical ports and airfields. They should disrupt our command and control infrastructure by damaging or destroying communications nodes or computer systems. They should attempt to destroy irreplaceable prepositioned equipment depots or ships as well as logistics support ships such as ammunition ships and oilers and airborne refueling assets. They should attempt to destroy or damage as much of the America's critical sealift and airlift assets as possible. In short NPC should use its SOF to make it as difficult as possible for the U. S. military to conduct business as usual.

NPC should attempt to establish contact and ultimate liaison with anti-American terrorist groups. In the case of foreign terrorists, this contact may be direct. Overt ties might lead NPC to being branded as a terrorist or rogue state, with consequent trade embargoes, and should be avoided. Contact with U. S. domestic terrorists should be done in ways that do not reveal the principals. Militia groups might be convinced to perform specific acts of sabotage and other disruptive activities. However, they would likely refuse to do so if they knew that a foreign government was behind the requests. Terrorist groups may be considered as adjuncts to any special operations forces NPC may possess and should be incorporated into overall planning.

Prior to the initiation of open hostilities, NPC may wish to employ some of its SOF to act like terrorists. Bombings and/or "random" attacks by small boats on naval forces around the world could serve to weaken U. S. forces just at those times when the U. S. needs to be strengthening its capabilities. Whether the attacks fail or succeed, NPC can deflect any blame and suspicion onto other known adversaries of the U. S.

The United States should increase its readiness to defend against adversary Special Operations Forces. Such readiness will as a direct consequence increase our ability to protect our forces and facilities against terrorist operations. Opposing Forces (OPFOR) activities should include a SOF element. Training exercises for units of all types and sizes should include scenarios that require defense against SOF. The Department of Defense should consider using elements of U. S. Special Opera-

tions Forces to test the defenses of our military facilities on a regular basis. This activity could conceivably be incorporated into the normal SOF training regime. If this is not deemed practical, then separate SOF units should be established (re-established, actually) to systematically review and test security forces, security equipment, and security procedures at U. S. facilities around the world. Such activities would help in defeating future actions by adversary SOF forces but also by terrorist groups.

LIMITED ADVERSE WEATHER OPERATIONS CAPABILITY

Weather can be a powerful, though fickle, ally. Allied forces took advantage of one-sided knowledge of a break in the stormy weather in the English Channel to successfully launch the Normandy invasion [108]. German forces had one-sided knowledge of an extended period of dense fog (grounding the Allied air forces) when they initiated the Battle of the Bulge [109]. Any adversary that has good knowledge of regional weather conditions will find occasions when it can use good weather or adverse weather to its advantage.

Currently U. S. naval forces do not conduct normal operations in sea states greater than 5 (Beaufort Force 6 [110]). They struggle to survive in sea states greater than 7 (Beaufort Force 10). U. S. forces will avoid sailing into hurricanes and typhoons if at all possible. Timing a military provocation to coincide with the presence of a violent storm between the location of the provocation and the nearest battle group will add significant delays to the on-station arrival of that battle group.

Adverse weather does not affect both sides of a conflict equally. Sensor systems using different signatures (e.g., thermal imaging versus television) will be degraded in different degrees as the weather worsens. Different platforms will have different mobilities as weather conditions change. Wheeled vehicles may be bogged down by mud that would not bother tracked vehicles. Rivers that were easily forded at one time may preclude crossing by all but amphibious vehicles after heavy rains cause them to rise. A helicopter assault may be prevented by strong winds that would have little effect on an equivalent armored vehicle assault. Detailed knowledge of weather conditions can allow an adversary to employ its assets in optimal fashion [111], [112]. If at the same time the U. S. lacks adequate weather knowledge, we would be forced to guess how to optimally employ our own assets. Even if both sides have equal knowledge, the side on the offense can choose to employ those assets and tactics that favor the offense given a known weather state.

Undersea warfare is one warfare area that is asymmetrically affected by adverse weather. High winds and correspondingly high sea states produce high underwater acoustic noise levels. This makes it difficult to detect submarines. High winds hinder flight operations (both fixed and rotary wing), restricting the scope of antisubmarine sweeps to surface vessels (and submarines) only. However, nuclear submarines are almost totally unaffected by surface weather conditions. The high acoustic noise will make it somewhat harder to detect surface targets, but not drastically. Thus, submarines could be used with much better effectiveness against our forces in adverse weather than in fair weather. Offensive mine warfare has similar asymmetries with respect to adverse weather.

U. S. knowledge of and ability to predict global weather is good [113] and will get better as more and better weather satellites are launched. However, the "goodness" in the Western Pacific is much worse than over the Continental United States, because satellite coverage is reduced. Much of the current quality in WestPac is due to international cooperation with Japan and other states that share land-based and sea-based weather measurements. If a conflict were to eliminate the sharing of weather data, U. S. prediction accuracy would fall dramati-

cally. It would fall even more dramatically if antisatellite weapons destroyed one or more of the few U. S. (or friendly) weather satellites. If an adversary can preserve its weather prediction capability while the U. S. loses its ability, then U. S. forces can be at a severe disadvantage. Not only will U. S. combatants be unable to predict local weather for military operations, but also logistics operations will be considerably less efficient and more hazardous when airlift and sealift platforms are no longer able to route their paths to avoid severe weather.

NPC should develop its own highly capable "Weather Service". It should deploy its own weather satellites (concentrating on NPC's landmass and its nearest ocean regions). These satellites should make maximum use of laser radar technology (for high-resolution 3-dimensional mapping of the temperature, pressure, humidity, and wind speed/direction -- the major drivers of weather change) [114]. NPC's Weather Service should develop and procure the infrastructure of computers and software models that will enable it to make long-term weather predictions at least as good as those of its U. S. rival. It should make every effort to incorporate the satellite laser radar data into those models. It should expend considerable basic R&D in the areas of basic meteorology and be an active participant in global meteorological studies. Emphasis should be placed on understanding the fundamental drivers of weather change with an eye to ultimate control of the weather. To ensure its superiority in forecasting the weather, NPC should plan on eliminating U. S. weather satellites (including those covering the U. S. itself) at the onset of a conflict.

Adverse weather should be considered as a possible tool to assist military operations. Military planners should be educated in the essentials of meteorology to facilitate that use. Any development in technology or use of asymmetric tactics that permits NPC to operate in adverse weather in which the U. S. cannot operate gives NPC a distinct advantage. This advantage is magnified if NPC has weather prediction capabilities accurate enough for it to plan to engage only during adverse weather. For example, NPC should develop its mine capability and submarine force with an eye to operation in adverse weather. Mines and submarines are not subject to the same wind & wave forces as surface ships. In addition, helicopter-borne mine warfare systems and anti-submarine warfare systems cannot be employed in adverse weather, although attacks with mines and submarines should be possible in all but the worst weather. Thus, if NPC sowed mines directly in the path of a battle group and simultaneously attacked the battle group with submarines during a full-blown tropical storm, the battle group would be at its most defenseless, while NPC's weapons would be minimally affected. NPC should also investigate technology developments facilitating adverse weather air and land operations. Covert terrain following/terrain avoidance sensors and precision bad weather landing systems can reduce the periods of time when air power is limited. Improved traction/suspension systems can improve mobility over adverse terrain such as steep, muddy slopes or deep dust/sand pits. Proper attention to these concepts could turn the weather from a neutral factor into an ally.

As knowledge of weather cause and effect improve, due to R&D advances, it may be possible to affect the weather directly. Causing devastating storms to strike some countries and not others, modifying rainfall patterns to ruin agricultural yields, and disrupting the normal flow of goods and services are ways in which weather can be a powerful strategic weapon.

Weather modification on a local scale has been attempted with varying degrees of success for many decades. Seeding of clouds with silver iodide crystals has been proven to increase local precipitation. It has also been proven to be incapable of significantly increasing precipitation if the proper conditions for such precipitation are not already in place. That is, cloud seeding cannot make it rain. It can only make it rain harder or rain sooner or rain longer than would normally occur. Nevertheless, considerable effort was expended on Project Popeye (initiated in 1966 and continued through 1972) to seed clouds in Southeast Asia.[112] The intent was to increase the magnitude and duration of monsoon rains along the Ho Chi Minh trail in the hopes that the increased muddiness of trails would slow the flow of war materials into South Vietnam. Although the results are equivocal, many believe the program had a major effect on North Vietnam's logistics abilities. The use of carbon dust to increase water vapor evaporation from bodies of water has also been demonstrated. Used together on a large scale, cloud seeding and evaporation acceleration might produce substantial modification to normal rainfall patterns. The dispersal of fog has also met with limited success. Large thermal generators can clear fog from airports, but the energy and equipment expenditures are seldom worth the results produced. Heating selected portions of thunderstorms with microwaves could prevent the formation of tornadoes.[115] Although technologically feasible, the expense of building a demonstration system (probably ten times the cost of the international space station) has prevented significant progress.

Weather modification on a grand scale is an enormous undertaking that is still science fiction today. The power dissipated in simple thunderstorms ranges from less than 10^{10} W for small highly localized storms to well over 10^{11} W in a large storm.[115] Total stored energy in thunderstorms are in the range of 10^{13} to 10^{15} J. The energy contained in a typical hurricane (10^{18}-10^{20} J) is comparable to that which would be released by 10,000 thermonuclear explosions (hydrogen bombs) [116]. The power dissipated by such a storm is of the order of 10^{13}-10^{16}W. Modifying such a weather event in real time would involve an expenditure of energy that was at least a substantial fraction of the total energy content at a power that was comparable to the dissipation rate. At a minimum we might expect that required powers of 10% and total energies of 1% would be needed. For a thunderstorm this implies gigawatts of power applied for many minutes (yielding a total delivered energy of the order of a terajoule). For a hurricane this implies terawatts of power applied for many hours (yielding a total delivered energy of many petajoules).

Exajoule energies at terawatt to petawatt powers (many terawatts for hours of cw operation) are beyond current human control (except in nuclear weapons, if they can be said to be controlled). However, the progression of time has given man the power to produce and use increasingly large energies and powers. Current technology in directed energy devices can produce gigajoule energies at megawatt powers (in cw systems operating for minutes). If sufficient justification were provided, current technology could be pushed by brute force to build microwave systems with gigawatt powers that could operate more or less continuously. A few decades ago we were capable of gigajoule energies at kilowatt powers (in cw systems capable of operating for months). In 50 years it is entirely possible that those pursuing the technology may be able to wield the requisite powers and energies needed to control the weather. As our understanding improves concerning the means by which large storms arise and how weather dynamics affect them, we may be able to trigger the occurrence of such storms or counteract their formation by appropriately modifying the initial conditions. This should require somewhat less power and energy than that required to control an existing storm. We may be able to substantially modify future weather long before we can control today's weather.

The Environmental Modification Convention prohibits offensive weather warfare [117]. The United States and many countries have signed this convention. However, it is likely that our NPC will not be a signatory to this convention. Several potential NPCs are not yet signatories. If NPC developed weather warfare capabilities, it would not be bound by treaty from employing it. Since the United States and most western powers are signatories, retaliation in kind for NPC use of weather warfare is effectively prohibited.

The U. S. should take steps to maintain its lead in weather prediction research. It should also invest in the improved weather satellites and other sensor that can facilitate improved weather prediction. The next generation of weather satellite might have several lidars and thermal sounders for 3-D measurement of wind velocity, temperature, pressure, humidity, aerosol content, and selected trace gas concentrations. The U. S. should orbit enough of these satellites to guarantee twice daily coverage of the whole earth even if satellite malfunctions or is destroyed. Research should also continue into understanding the causes and dynamics of the weather. This will not only improve our prediction abilities but also lay the groundwork for future weather modification efforts.

The U. S. should also have a program of regularly evaluating whether technology has progressed to the point that weather control is becoming possible. At the earliest evidence of near-term feasibility, the U. S. should institute programs to convert the feasibility into reality. The U. S. cannot afford to let an adversary gain a monopoly on weather control.

The U. S. should also consider new designs for its military platforms that incorporate increased adverse weather capability. For example, there is no fundamental reason why aircraft cannot regularly operate safely in "zero-zero" conditions (zero visibility, zero ceiling) or in gale force winds. There is no fundamental reason why amphibious operations cannot safely be undertaken in Sea State 8. There is no fundamental reason why a missile attack cannot be safely initiated and executed in the worst stages of a tropical cyclone. Radical new approaches and designs would be required, but the payoff of insensitivity to weather would negate any adversary attempts to use the weather as a tactical weapon against us.

The U. S. should also pay attention to the principle of "weather complementarity" when it acquires and deploys its systems. If one component of a military force is severely limited by one form of weather, then an ancillary force component should be included that is not limited by that form of weather. For example, since all surface combatants are limited by sea states greater than 6, carrier battle groups, deployed in situations where such sea states might be encountered and used as an *advantage by an adversary, should be accompanied by a substantially increased complement of attack submarines*

ATTACK BY NONLETHAL WEAPONS

An adversary may choose to employ nonlethal weapons in some of his access denial operations. See Appendix K for a technical discussion of nonlethal weapons. ***In all likelihood, these weapons would be used by "civilian" entities. In the late stages of a crisis or early stages of open hostilities, the adversary will wish to delay the arrival of U. S. military assets into the trouble spot. Nonlethal weapons could effect this result without necessarily resulting in escalation. For example, early in a crisis situation an adversary employs nonlethal weapons in an attempt to delay our forces from arriving in theater at a specific time. Adversary-sponsored "civilian protesters" using a fleet of small ocean-going craft confronts a battle group at a choke point with anti-mobility weapons (propeller fouling nets or turbine-fouling polymer aerosols) and/or anti-materiel weapons (non-nuclear EMP devices or metal embrittlement agents). If the adversary action is successful, a significant fraction of the battle group may be incapacitated for one or more days. The entire battle group will likely be forced to delay until damages can be repaired.***

The problem for U. S. forces is how to respond? Do they use lethal force to quickly negate the threat and resume progress toward the area of conflict (and face near-universal public condemnation and possible future charges of war crimes)? Do they change course to avoid the protesters (and add many hours to the arrival time – allowing the adversary to achieve his objective of delay)? Do they maintain position and await the arrival of forces more suited to police action (again allowing the adversary to achieve his objective of delay)? Do they sail into the civilian force and hope that the "civilian" tactic was a bluff? If it wasn't and the nonlethal weapons effectively disable a number of ships in the battle group, how do the U. S. forces respond? Do they take retaliatory action? Do they let the "civilian" fleet retreat and remain able to repeat the confrontation in the future? How do they repair the damage, and if possible, get the group underway again in a timely fashion? How do the answers to the above change if there is no crisis situation (and the confrontation is merely a test of will), or if the crisis situation has escalated to hostilities, or if general war has been declared between the U. S. and the adversary.

In another scenario, a civilian aircraft discharges a cloud of super-lubricant mixed with graphite fiber chaff, in front of the battle group. As the cloud passes over the battle group, the decks and superstructures become thoroughly contaminated. Countermeasures washdown systems (if activated at all) force immediate abort of all deck operations and are not 100% effective in either their coverage or their removal of the larger particles composing the cloud. The super-lubricant makes it unsafe to conduct any operations above deck. Personnel cannot walk safely on any combatant. Aircraft cannot be safely maneuvered on flight decks (especially the one on an aircraft carrier). The graphite chaff immediately shorts out some antennas with high field strengths. Over time the smaller graphite fibers find their way into the interiors of electronic boxes and short out critical components. The super-lubricant makes repairs and decontamination almost impossible. The battle group may be out of action for days.

What sort of response is practical in this scenario? Shooting down the civilian aircraft is an option (but only after the attack has begun) and may be nothing more than an act of revenge (the attack may be over before shootdown occurs). However, it may not be possible to unequivocally determine that an attack is taking place. Furthermore, since the attack is nonlethal, shootdown is probably not an option for subsequent attacks. Lethal response to an attack with known nonlethal consequences would likely be deemed unacceptable. Maneuvering away from the cloud would delay arrival, an acceptable outcome for the adversary. What tools are available for remediation? Nothing but water and elbow grease.

Consider another scenario in which a peacekeeping force is "attacked" with malodorants (stink bombs), riot control agents (such as tear gas), or calmative agents, thrown from a crowd, from windows and roofs overlooking streets, or from behind fences. The peacekeeping force would be forced to go to MOPP 4 (full chemical protective gear). Repeated attacks can prolong this state indefinitely causing the peacekeeping force to restrict its activities to avoid overheating. Patrols become more limited. Even encampments are not safe from wind-carried agent attacks. Peacekeeping force presence in the region is reduced to levels that ultimately lead to failure of the peacekeeping process. How does the peacekeeping force respond to this threat? Lethal force would not be justifiable. Employment of U. S. nonlethal weapons is an option but may not prove to be an effective countermeasure. Improved protective systems are not readily available.

Consider a third scenario in which a coup threatens stability in a third world country and a non-combatant evacuation operation (NEO) is undertaken. As helicopters land security forces in obvious staging locations, the helicopters are disabled by EMP guns, preventing timely withdrawal. Super-lubricants, sticky foam, or nets hidden in aqueous foam entrap or otherwise prevent the security forces from moving to accompany the non-combatants and prevent the non-combatants from moving to join the security forces. Another set of microwave weapons is used to cause overheating in the security forces, further their ability to resist. One set of potential hostages has thus been joined by a second. What can be done to prevent such a scenario? Again use of lethal force is neither justifiable nor even practical. Hardening of equipment against EMP is expensive and seldom done thoroughly. Tools for breaching "nonlethal" barriers are not available.

The last two scenarios are not really access denial scenarios. However, effective anti-power projection capabilities indirectly support access denial by forcing limited resources to be spent addressing them that could otherwise be spent on countering access denial systems. Furthermore, any vulnerability of our forces is still a vulnerability even if it does not directly impact access denial.

The lack of serious discussion of these possibilities and of potential courses of action indicates that the U. S. does not have (or has not promulgated) definite policies on how to respond to such unconventional attacks. It also lacks tools to address these new weapons and modes of attack. All of our military forces (land, sea, and air) generally lack nonlethal weapons to counter forces employing nonlethal weapons against them. Those forces generally lack defenses against such weapons (you don't develop defenses against threats that have not yet been recognized as being serious). The forces also lack remediation measures against these

threats. For example, if the enemy were to employ turbine-fouling polymer aerosols, solvents capable of rapidly dissolving or neutralizing the polymer are almost certainly not carried on board the target vessels. The fact that nonlethal weapons are not likely to be used against U. S. forces in a full intensity conflict does not mean that they are not significant threats in any situation short of lesser intensity conflict.

NPC should consider the development and deployment of nonlethal weapons technologies. It should concentrate on those weapons with military applications, unless internal political stability requires the development of improved crowd control and riot control agents. To employ the militarily significant NLWs, NPC should create a "civilian" front organization that could legitimately justify possession and use of such weapons. Civilian use of NLW is more likely to cause ethical problems for the U. S. commanders than military use of the same NLW. NPC should ensure that sympathetic individuals from the world media are present at all events staged by the civilian front. The front organization should be staffed to adequate levels, militarily trained, and supplied with appropriate platforms (fishing boats, pleasure craft, coaster trade vessels, etc.) for deploying the NLWs. The front organization should occasionally engage in activities that would publicly justify its existence and solidify its "legend".

NLWs of potential access denial significance include:

- entanglements (such as steel reinforced nets towed between small craft),
- filter clogging agents (aerosols dispensed from spray tanks or mortar-fired airburst projectiles),
- biological fuel-eaters (aerosols dispensed from spray tanks or mortar-fired airburst projectiles), and
- anti-materiel agents (also dispensed as aerosols from spray tanks or mortar-fired airburst projectiles). Among the potential anti-materiel agents are metal embrittlement agents, superacids, and polymer modification agents, all of which would degrade shipboard equipment to unusable states.
- anti-personnel agents (also dispensed from spray tanks or mortar-fired airburst projectiles). Among the potential anti-personnel agents are calmative agents, irritant agents (riot control gases), and malodorants. Anti-personnel agents are most likely to be useful in a harassing role. Ships would be forced to activate collective protection systems. Personnel in unprotected areas would be forced to wear chemical agent protective gear.
- Anti-traction agents (also dispensed from spray tanks or mortar-fired airburst projectiles) could make it unsafe to conduct any operations above decks.

NPC is likely to find useful NLW applications in areas other than access denial. These should also be investigated.

The U. S. has explicit doctrine governing use of nonlethal weapons by our military against civilian and military forces of other nations [118] and it continues to refine both doctrine and tactics in this area. However, it needs to develop doctrine addressing adversary employment of nonlethal weapons against U. S. forces. The possibility of such use should be included in contingency planning. The U. S. should treat significant NLW developments in the same fashion as conventional *weapon developments. Intelligence should be acquired concerning potential NLW deployment. Tactics for making NLW employment more difficult need to be developed. Defenses should be developed against the more serious NLW developments, as should means for remediation of the effects of adversary employment of those weapons.*

CHAPTER 8. ATTACKS ON LOGISTICS RESOURCES

LIMITED STRATEGIC SEALIFT/AIRLIFT CAPABILITY

The United States lacks the sealift and airlift capability to rapidly deploy an overwhelming force. At best, one light division of airborne troops, one battalion of marines, one carrier battle group, and/or one composite air wing can be deployed and in combat within a few days. Few follow-on forces could be employed in combat without at least a one-month notice. Many would require several months notice. The primary reasons for this are deficiencies in numbers of fast sealift ships and heavy airlift aircraft. Should something affect the readiness or survivability of these assets, the U. S. ability to project ground forces would be seriously degraded. Both sealift and airlift capabilities are limited by numbers of platforms. Every cargo ship or aircraft that can be made non-operational is effectively irreplaceable. The platforms themselves thus become high-value targets. When loaded with critical war materiel, they are even higher value targets. These high-value targets nevertheless rate near the bottom of the priority list in receiving aircraft survivability equipment (such as radar warning receivers, self-protection jammers, and flare and chaff dispensers). As a consequence they are vulnerable to shoulder-fired surface-to-air missiles (SAMs) during both takeoffs and landings (at every airport) and to interdiction by long-range SAMs and fighter aircraft in the theater of operations. They are also vulnerable to sabotage and special operations force attacks on airfield facilities.

In theory the U. S. can augment its air transport capability by exercising its Civil Reserve Air Fleet (CRAF) contracts with commercial carriers [119]. This can provide a large quantity of troop transport aircraft and cargo aircraft by "drafting" civilian airliners into military use. However, if a major conflict were to erupt overseas, the need to transport the majority of our armed forces overseas in the shortest possible time would require calling up every available aircraft. As more passenger aircraft are withdrawn from air charter flights and ultimately scheduled airline service, the American public will be more and more severely affected. Business and pleasure travelers may be forced to wait days for flights because the American flag carriers have all of their long-haul airliners diverted to carry troops. Businesses will not get their accustomed overnight package delivery because the express air carriers are transporting military equipment. These acts will ripple through the civilian sector, affecting producers, retailers, service providers and their employees alike. The economy will suffer and public opinion may significantly shift away from support of the military operations.

The civilian assets that are drafted into service will not have even the minimum defensive assets possessed by military airlift aircraft. A C-5 or C-17 may be provided with flare dispensers to protect against shoulder-fired surface-to-air missiles (SAMs) and their pilots may be trained in evasive maneuvering; commercial aircraft will not have flare dispensers and their pilots may have not received missile attack training. They will be much more vulnerable to air and surface-to-air missile attacks when they arrive in theater.

The whole augmentation scheme can be co-opted by a pre-meditating adversary. It is possible for adversary "companies" to book large numbers of charter aircraft for the time frame when the adversary anticipates starting hostilities. The charters would be flown overseas on valid prepaid contracts and simply be unavailable and untouchable when the U. S. government needed to commandeer them. The same preemptive actions could be taken with commercial cargo aircraft. The net effect would be to hasten the need to commandeer scheduled airline and express delivery assets, with the attendant disruptions of the American lifestyle and economy. American Merchant Marine ships can be pre-empted in a similar fashion, reducing the availability of secondary sealift assets.

Any surge in strategic sealift and airlift requires more than just available aircraft and ships. Ports and airfields are required at both ends of the logistics chain, trained personnel are required to load and unload the ships and airplanes, and fuel to run those ships and airplanes is needed at specific critical locations. An adversary can reduce America's strategic lift capability by striking at any of these requirements. Ports and airfields can be attacked with missiles, special operations forces, or weapons of mass destruction. Longshoreman can be kept from working by chemical or biological weapons. A simple outbreak of virulent influenza might never be traced back to the adversary, but could cut throughput in half. Fuel supplies can be destroyed, or contaminated so that all fuel must be laboriously checked before use. Fuel supplies can also be adversely affected by preemptive actions. Consider oil supplies at a critical overseas port. In the weeks before the conflict adversary merchant ships in large numbers visit the port and draw off as much fuel as they can hold. They pay top dollar for the extra fuel consumption. At the same time, other adversary companies conclude lucrative deals with the major fuel suppliers to that port that result in "temporary" reduced fuel deliveries and delays in fuel deliveries – premium prices are paid for priority deliveries to ports unimportant to the coming conflict. Increased demand and decreased supply results in a major drawdown of stored reserves. When the conflict starts, this port can no longer support the rate of operations needed by U. S. strategic sealift.

Unless NPC has the ability to negate the strategic sealift and airlift capabilities of the United States, then NPC should undertake no military action or sequence of military actions that cannot be brought to a satisfactory and definitive conclusion within four to six weeks. If such brief yet definitive operations are not deemed practical, then NPC must investigate and develop capabilities to interfere with the U.S. sealift and airlift capabilities.

Options for disruption of strategic lift include sabotage (of individual platforms or loading/embarkation facilities), disruption via information warfare (viruses or semantic attack), and in-transit interdiction (via submarines, surface action groups, long-range aviation with in-air refueling capability, or theater aviation). Other options include denial of secure landing and/or debarkation facilities (via airfield or port destruction, WMD agent contamination, or capture), preempting of civilian assets (via pre-meditated charters and relocation), terrorist/special operations attacks (with short-range anti-armor or anti-aircraft missiles), and reduction of strategic fuel supplies (by preemptive redirection, direct attack, or contamination). In all likelihood, NPC will need to pursue several of these options. The choice should be coordinated with NPC's grand militarization strategy to maximize the procurement of multiple use assets (such as long-range aviation or submarines).

With the exception of preemptive activities, disruption of U. S. strategic sealift and airlift should be carried out on the same time schedule as the lift activities themselves. The most aggressive and massive attacks should occur when the most lift assets and cargoes are at risk. Every attempt should be made to force maximum reliance on CRAF and Merchant Marine assets. Such reliance will have adverse effects on the American economy and public opinion.

The U. S. has a definite shortage of heavy lift aircraft and sealift ships. It should pursue acquisition of further quantities of heavy lift aircraft such as the C-17 or its potential follow-on. It should actively pursue the development and acquisition of a number of high-speed, large gross displacement, roll-on/roll-off cargo ships. A reasonable objective might be the acquisition of enough strategic lift assets to permit rapid deployment of one next-larger military unit than each element is current capable of deploying. For example, if we currently have the ability to airlift one light division into a theater within 48 hours, then we should acquire the assets to permit deployment of an armored division (or a corps of several light divisions) in the same time frame.

The U. S. needs to take measures to assure the survival of its airlift and sealift assets. Military aircraft should be provided with state-of-the-art electronic warfare systems including active jammers and decoys in all portions of the electromagnetic spectrum. Civilian aircraft drafted for airlift purposes should at a minimum have decoy dispensers. Given the growing threat to civilian airliners from handheld surface-to-air missiles (SAMs, such as SA-7, SA-14, SA-19, Stinger, etc.) wielded by terrorists, the U. S. should give some thought to placing missile launch warning detectors and flare dispensers on all civilian transport aircraft, even in peacetime. In the period from 1978 to 1993 there were 28 attacks in third world countries on civilian aircraft by terrorists using hand-held SAMs. It is only a matter of time before such terrorism invades the borders of the United States. Whenever, large flights of transport aircraft are underway in the same region, consideration should be given to providing them with fighter escorts. Aggregates of strategic airlift assets might make attractive and high-priority targets for adversary air forces (even those with limited numbers of combat aircraft). Perhaps a convoy system should be employed for air transport.

Sealift assets also need protection. If a potential adversary has a significant submarine force with some blue water capability, sealift assets could be at risk from the moment they leave port. Escorts and convoying clearly need to be considered. Any ships used for escort duty should have organic minehunting capabilities. Limited missile and torpedo defenses might also be in order. Electronic warfare systems can be packaged in containers that could be lashed to the decks of transports to provide detection and jamming. Defensive missile systems such as SeaRAM could be similarly packaged in self-sufficient units that could be loaded on-board prior to departure, as could towed anti-torpedo decoys.

Facilities that service the airlift and sealift assets should be protected against attack by special operations forces or weapons of mass destruction among other threats. Adequate facilities and expendables need to be available for rapid neutralization or remediation of the effects of any such attack.

RELIANCE ON LIMITED OVERSEAS BASING

In the latter half of the 20th Century, the United States enjoyed a luxury of having multiple overseas bases in more than a dozen countries. A large part of our armed forces were stationed in the regions where it was anticipated that they would fight their next battles. The changing world environment is now forcing the United States to withdraw more and more of its military forces from its overseas bases. Some bases (and countries) have been abandoned entirely, either because they are no longer needed, because we can no longer afford to maintain them, or because the United States military is simply no longer welcome there. The majority of these former bases are now unavailable for future U. S. use. Despite this the United States still has a number of critical overseas military installations, although some reductions will continue for many years. Negotiations for closure or partial withdrawal are far more numerous than negotiations to open new overseas bases. The United States military is not equipped to mount all of its military operations from bases restricted to the United States proper or its territories. Every overseas base surrendered or abandoned reduces the combat effectiveness of the United States in that region of the world.

Some of the most critical bases (e.g., Guam and Diego Garcia) are weakly defended. They are isolated with no nearby bases to offer mutual defense (Guam and Diego Garcia are on remote islands). They have limited permanently assigned air, ground, and naval defensive forces with limited air defense and no long-range ballistic missile defense. It is not unreasonable to assume that these bases could be quickly neutralized by ballistic missile strikes, cruise missile attacks, airborne assaults, amphibious invasions, harbor mining, or combinations of the above. Several potential competitors are developing ballistic missiles with sufficient range to strike these bases. Critical facilities at these bases could be easily destroyed in attacks by special operations forces. Even worse would be direct occupation by adversary airborne assault or maritime assault forces. Prior to the outbreak of hostilities, a single battalion of assault forces would probably suffice to subdue the local defense forces at many of these bases. In adversary hands, Guam and Diego Garcia could provide outposts allowing extension of access denial capability far beyond the nominal 1000-2000 km range. Additionally, bases located in stable, friendly countries (e. g., Yokosuka, Japan or Incirlik, Turkey) are not so strongly defended that they are immune to devastating attack. Even bases in the United States are not completely secure, although the same long distances that force the U. S. to have overseas facilities make bases in CONUS somewhat less vulnerable to attack.

NPC should make every attempt to eliminate any U. S. overseas bases that could be of use against it. It should exert diplomatic and economic pressure on governments that permit U. S. basing. Economic incentives including investment, direct foreign aid, and bribery should immediately flow from NPC to any country in the region that rejects U. S. basing when requested or evicts U. S. forces from existing bases. NPC should support insurgent groups in countries permitting U. S. basing with the proviso that those insurgent groups make U. S. presence one of their political issues. In the United Nations and other world forums NPC should protest U. S. overseas basing as being anachronistic imperialism and totally unnecessary in the new world order. NPC should make it clear to all offending governments that if hostilities arise, the overseas bases <u>and</u> the countries in which they are located will become priority military targets.

The NPC military should develop plans to neutralize (with any appropriate weapons) all U. S. bases located within its denial areas. This should include not only permanent bases but also any temporary facilities usage. Bases outside the denial area but close enough to support rollback operations should also be targeted. Especially critical bases such as Guam and/or Diego Garcia should be attacked with sufficient force to deny their use to the U. S. for the duration of the conflict. Ports and bases located in countries friendly to the U. S. but within the denial areas should be similarly destroyed, even if it strains relations with relatively strong countries such as Japan or Italy or Germany. Such base destruction should be conducted as soon as possible after the beginning of hostilities. However, any appearance of another Pearl Harbor should be avoided. Designated and proclaimed denial areas should extend at least as far away from any NPC territory as the range of a Tomahawk missile, and possibly farther. This will force any and all retaliation on NPC to be initiated from mobile platforms or extremely distant bases.

The U. S. should enter into whatever negotiations are required to reverse the trend of reductions in overseas basing. It should strive to have adequate basing in at least two different countries in any major geographic region. This will prevent a single change of heart on the part of a basing partner (as happened in the Philippines) from denying the U. S. any bases in a key geographic region. On a regular basis, every potential trouble spot should be reviewed to determine the suitability and adequacy of forward basing in the region.

The defenses at all overseas bases should be bolstered. All aspects of physical security should be addressed. Air and missile defenses should be increased to where they are capable of blunting the largest credible attack. Garrison forces should be increased to a size capable of repelling a major airborne or amphibious assault. Availability of NBC defensive measures should reflect the high probability of attack associated with such weapons. Increased defensive capabilities will reduce the possibility of terrorist attacks and will also reduce the likelihood of crippling attacks by any serious adversary.

RELIANCE ON PRE-POSITIONED EQUIPMENT

It is easier to rapidly transport personnel and their personal gear from U. S. bases to crisis areas overseas than it is to transport the heavy equipment, ammunition, and pre-packaged rations needed by those personnel after they arrive. Coupled with the previously mentioned deficiency in strategic lift, this is forcing the United States military into becoming more reliant on pre-positioned equipment to support its readiness objectives. A large fraction of the U. S. Army's heavy equipment is pre-positioned at land bases in areas where the probability of conflict is (or was) very high (Europe, Korea, and Persian Gulf) [120]. It is anticipated that by 2003 all of the equipment for eight heavy combat brigades of the United States Army will be deployed on 15 pre-positioned ships in the Pacific and Indian Oceans [121]. These ships constitute the Army Pre-Positioned Set-3 (APS-3). Most of the equipment for the Marine Corps' expeditionary brigades is already pre-positioned in this fashion. The U. S. Marine Corps currently has 13 (to be increased to 16) pre-positioned ships organized into three active squadrons (MPSRON 1,2 & 3 each with equipment for a Marine Expeditionary Brigade) [59].

Although pre-positioning cuts weeks off of deployment times, it creates a significant vulnerability. This critical warfighting materiel is transported on what are essentially merchant cargo ships that are crewed by contract mariners (although there is a small naval detachment aboard each ship). In peacetime these ships are either anchored offshore at some port within their forward deployment area or they sail around that forward area with minimum security, no self-defense weaponry, and no naval escort. Even the most inept submarine crew or missile boat crew could sink a number of these ships in a single engagement. A cell of well-trained terrorists could board any of these ships (in port or at sea), overcome the crew, and either scuttle the ship and its equipment or hold it hostage. Once hostilities appear imminent, the ships will deploy toward friendly ports near the potential conflict area. This transit towards hostilities may or may not be escorted by warships. However, it would be surprising if such an escort exceeded more than a couple of destroyers per squadron. If present, an escort might discourage an attack by a patrol boat or a single submarine, but a devastating attack is still not ruled out, especially if the attacking force is substantial. In peacetime, the land-based pre-positioned supplies are typically guarded by small, lightly armed forces that are not at the highest state of readiness. Any competent special operations force could overwhelm these guard forces and destroy or sabotage much of the stored equipment. After hostilities have commenced, despite increased alertness, the size of the protective forces would not be large enough to prevent a successful attack by a company-sized unit of paratroops (although the survival of the attackers could not be assured). Nor could any reasonable protective force prevent destruction of the equipment by an air or missile raid.

The trend towards increased pre-positioning will reduce the overall significance of the cargo of any one ship or storage facility. However, we will undoubtedly increase pre-positioning at the expense of having substantial reserves of equipment at home. Thus, the pre-positioned equipment will be irreplaceable on any time-scale shorter than many months. Loss of a substantial amount (20-40%?) of equipment from a single squadron could prevent an entire brigade from joining the fighting for weeks, if ever. Some of the component units (those

whose equipment was not lost) might be reorganized into one or two ad hoc battalions or could be attached to other brigades, but this will take time and full combat effectiveness will seldom be achieved. Making up the equipment loss by shifting the deployment of another squadron will take weeks at a minimum, and will reduce military options in the theater to which that squadron was assigned. Any attempt to increase the security of these ships by routinely assigning them naval escorts will further tax an overextended surface combatant force. If implemented only in times of crisis this would likely slow down deployment times by the amount that the prepositioning ships must wait for the escorts to arrive from their prior assignments.

NPC should develop forces capable of targeting and destroying the prepositioning ships located in its geographic region. Submarines, motor torpedo boats, missile patrol craft, aircraft armed with antiship missiles or gravity bombs, special operations forces, or even small trading or pleasure craft dispensing mines could accomplish the destruction. It is entirely possible that the prepositioning ships can be attacked as just one more type of mission for assets that are acquired for other purposes. This mission should be considered when total force structure requirements are determined.

NPC should establish a doctrine that these ships will be attacked at the onset of any hostilities between itself and the United States. NPC may also wish to consider a long-term program of covert or surrogate action against these ships. Sinking one ship with an untraceable WWII-vintage mine, crippling another in a terrorist attack several months later, damaging or even sinking a third in an "accidental" collision with another merchant ship a few months after that, losing a fourth to a hijacking by armed "pirates" in an area known for this kind of activity, sinking a fifth by sabotage in the port of a nation friendly to the United States, and so on, could severely limit the future warfighting capability of the United States without incurring any significant risk to NPC. Every ship lost would take years to replace without major military budgets increases specifically aimed at their replacement. The equipment lost would take similar lengths of time to replace.

If neighboring states have permitted pre-positioning of U. S. military equipment on their territories, then NPC should plan to attack and destroy the pre-positioned equipment storage facilities and their contents. One option is to attack these sites immediately prior to commencing hostilities by using special operations forces. These forces may destroy the stored equipment or may sabotage them in a fashion that would inflict great damage to any force that attempted to use it. Another option is to target the sites for air strikes or missile attacks. A final option is infiltrate a small special operations force during peacetime to attempt to destroy some or all of the facility while making that destruction look like an accident or the work of a local terrorist group.

It is doubtful that the U. S. can eliminate its reliance on pre-positioned equipment. Defenses at the land-based pre-positioning sites are almost certainly in need of significant enhancement. The defenses should be capable of surviving ballistic missile and/or cruise missile attacks, including use of chemical or biological weapons. They should also be capable of surviving at least company-sized attacks by special operations forces or paratroops. If pre-positioning compounds are not currently under the protection of corps-level ballistic missile defenses and air defenses, *then provision should be made to increase protection to those levels. Garrison forces protecting the compounds should be at least company strength, should be housed within the protected compounds and have the ability to obtain company-sized reinforcements within minutes.*

Critical mobile assets such as the pre-positioning ships also deserve protection. At a minimum, they should be provided escorts at all times. Such escorts could be destroyers or they could be attack submarines. In either case, more ships are required in the active fleets to be able to spare ships for escort duties. Consideration should also be given to providing the pre-positioning ships with minimal self-defense capabilities against missile and torpedo attacks. Electronic warfare suites including active jamming coupled with two or more Rolling Airframe Missile launchers might suffice for missile defense. Towed and expendable decoys might suffice for torpedo defense. It is recognized that such defenses would require increases in the size and changes in composition of the permanent Navy detachments aboard each ship. This would be a small price to pay to preserve the irreplaceable cargo carried on board.

RELIANCE ON UNDERWAY REPLENISHMENT

Carrier battle groups consume enormous quantities of fuel, food, and ammunition. When conducting combat operations the consumption rates increase significantly. For example, during combat force projection operations a Nimitz-class carrier can expend its entire stores of ammunition and aviation fuel in 2-3 days. Most combatants will require refueling after transiting at high speed from their homeports. The United States has only a small number of ammunition ships and oilers. Currently the United States has 4 active duty and 6 MSC ammunition ships (AE); 5 active duty and 15 MSC replenishment oilers (AO); and 8 active duty (plus 4 under construction) combat support ships (AOE) [59]. There is nominally only two active duty ships (1 AE + 1 AO or 2 AOE) plus one or two assigned MSC ships for each deployed carrier battle group and/or amphibious ready group. Each replenishment ship supports several combatants. Since these ships are lightly armed and transit unescorted between resupply depots and replenishment points, they too represent an extreme vulnerability.

One submarine could hypothetically eliminate all of the replenishment capability available to a theater of operations. The loss of any one of these ships can reduce the sustainable operations rate of a battle group by as much as 25-33%. The loss of several replenishment ships in a given theater of operations could result in almost complete operational shutdown. Without replenishment of fuel and ammunition, not only are offensive operations threatened, but also the ability of the battle group to defend itself becomes questionable. Aircraft without aviation fuel cannot fly combat air patrols (CAP) to screen the battle group from air attack. Ships without bunker oil cannot maneuver to prevent submarine attacks. Replacement of losses by further drawing from the MSC fleet is possible but would likely take many days to achieve. Besides, the MSC fleet assets are as limited in number as the active fleet. Replacement of lost replenishment ships out of the MSC fleet will prevent their use to support follow-on force deployments.

NPC should develop a strategy for targeting and attacking the replenishment fleet of the United States. The replenishment fleet should be among the first U.S. assets targeted. Any Military Sealift Command ships or ships taken up from trade (STUFT) to replace damaged U. S. replenishment assets, should also be made priority targets. At the very least, this would force the U. S. to devote a substantial fraction of its limited combatant forces to escort duty, weakening battle group strength. Risk to NPC forces would be small at best. It might also be desirable to use covert operations similar to those described in the section on pre-positioned forces. “Accidental” loss of a small number (3-5) of replenishment ships in the months before hostilities begin will place added strain on an already weak system. The low priority placed on logistics ships relative to combatants may preclude replacement shipbuilding programs from being instituted in a sufficiently timely fashion.

An extremely viable option for destroying the replenishment fleet is the development of nuclear attack submarines that are capable of independent hunter-killer operations in blue water anywhere from the resupply depots to the replenishment points. Diesel submarines supported by submarine tenders could be used to block traditional choke points. Alternative options for attacking the replenishment fleet include traditional sabotage, chemical/biological attack, or merchant ships flagged to neutral countries and equipped with simple radars and multiple short-range antiship missiles, or better yet, torpedoes. A complete missile or torpedo launching and fire control system could be hidden inside a standard shipping container. In the case of using torpedoes, the launch would go completely undetected and the cause of the sinking might never be discovered. The SLQ-32 electronic warfare suites on board the replenishment ships would probably give early warning of a missile attack, although if three or four missiles were launched simultaneously, the probably of the ship's defensive weapons defeating them all is very small.

The U. S. cannot eliminate its reliance on underway replenishment. The design of ships capable of operating without support for months would be impractical. Although we have done so for submarines, there are cost penalties such as reliance on nuclear propulsion. Furthermore, even a nuclear attack submarine must obtain replacement ordnance on a regular basis if it is actively engaged in a large-scale shooting war.

Since it is not practical to eliminate underway replenishment, the U. S. should take actions to preserve an underway replenishment capability. More oilers and ammunition ships are needed to act as replacements for combat losses. Reserves should be capable of replacing almost every deployed ship at least once. To avoid the delays associated with activation of reserves, the number of active duty replenishment ships should be increased. Critical assets such as the replenishment ships deserve protection. At a minimum, they should be provided escorts to and from the forward areas and resupply ports. Such escorts could be destroyers or they could be attack submarines. In any case, more ships are required in the active fleets to be able to spare ships for escort duties. The replenishment ships should be given minimal self-defense capabilities against missile and torpedo attacks. Electronic warfare suites including active jamming coupled with two or more Rolling Airframe Missile launchers might suffice for missile defense. Towed and expendable decoys might suffice for torpedo defense. It is recognized that such defenses would require increases in the size and changes in composition of the permanent Navy detachments aboard each ship. This would be a small price to pay to preserve this essential warfighting capability.

CHAPTER 9. ATTACKS ON SOCIETAL VULNERABILITIES

CIVILIAN INTOLERANCE OF CASUALTIES

In the minds of the American public, the 1960's, 1970's, and early 1980's military operations in Vietnam, Lebanon, and elsewhere, produced high levels of casualties in conflicts of questionable merit. This can be contrasted with the successful operations of the late 1980's and 1990's. Many people believe that the "pointless loss of life" in Vietnam contrasted with the "almost bloodless" Gulf War has left the American public with an expectation of low casualties and a consequent intolerance of any casualties at all in military operations. It is perceived that public support for a military operation tends to fall with each casualty. If an operation incurs too many casualties in a cause that is not universally acclaimed as being in the vital interests of the nation, it will likely be abandoned before successful completion. At a minimum, public opinion will be turned against the military, and will result in decreased support for future operations and sustained military budgets.

The truth of this perception will not be argued here. However, the existence of the perception tends to produce self-fulfilling prophecies. As casualties mount in an operation, the press will dwell on the carnage, predict more casualties in the future, and raise the issue of whether it is in our best interests to continue the fight in light of the casualties. The self-doubt this in turn raises in ourselves will make us less tolerant of additional casualties, unless our moral certainty in the correctness of our cause is equally reinforced. Most of the press reports will emphasize the casualties, not the morality of our cause. Some will question the morality of the cause if it leads to warfare, regardless of the true nature of the cause. Ultimately, we will tire of the strife and call an end to things unless victory is in sight.

Both moral certainty of the need to fight and the probability of ultimate victory are necessary to sustain our motivation to fight. No one questioned the moral aspects of World War II, even when the war was confined to Europe and China. America opted not to fight until after it was directly attacked by Japanese armed forces. Our need to join the fighting was not viewed as sufficiently strong. In World War II, victory in the Pacific was perceived as inevitable by many as early as June 1942 (after the massive defeat of the Japanese navy at Midway – success on Guadalcanal later in the year served to reinforce that conclusion). In the European Theater, the success of the North African landings pointed the way to ultimate victory over Germany at almost the same time. For most (at least 2½ years out of 3½ years total) of the American segment of WW II, ultimate victory was viewed as inevitable. This made it possible to continue fighting even though the losses became heavier as the war neared a conclusion. In Korea, after the Chinese entered the fight on the side of the North Koreans, the war stagnated into repeated bitter fighting over small pieces of territory. As the likelihood of ultimate victory diminished, American public opinion turned to accepting a stalemate maintaining a divided Korea. In Vietnam, the actions of the U. S. government soon made it clear that we were fighting to maintain a status quo, not to achieve victory. The inability to see a successful conclusion to the fighting led to the cascading concern over pointless casualties.

Any adversary that can inflict heavy casualties on U. S. forces and deny us any clear-cut path to victory, will in all likelihood be able to force a stalemate, if not obtain a nearly complete victory.

The American public aversion to casualties is especially strong if those casualties are caused by "friendly fire", that is, fratricide [122], [123]. Historically, fratricide has accounted for 10-25% (average of 12%) of all casualties in every major engagement since World War II. In Desert Storm, fratricide accounted for 24% of American fatalities and 15% of all wounded [123]. Despite foreknowledge that fratricide is commonplace on the battlefield, every major fratricide incident seems to lead to a public hanging of the "guilty" party. Americans also have an aversion to causing casualties (even unavoidable ones) among "innocent" civilians. This aversion is almost as strong as that to fratricide. The general results of fratricide and civilian casualties are very restrictive rules of engagement. The effects of such rules are discussed in the next section.

NPC's basic strategy should exploit America's intolerance for casualties. Any selective transparency into NPC military capabilities should make it obvious that any military intrusion into NPC affairs will result in substantial U. S. casualties. The continued, visible existence of a massive, capable land army in China unequivocally demonstrates the potential success of this strategy. The continued strength of the Chinese army coupled with the U. S. experience in the Korean conflict and Vietnam has led to the current military dogma that the United States will never again become involved in a land war in Asia (outside of fighting to maintain the status quo in Korea). NPC strategy should also ensure that early confrontations with the U. S. should produce either no casualties or major casualties. Zero casualties gives each side the ability to disengage with honor. Major casualties may trigger the public reaction that would force U. S. withdrawal. The NPC should not wait until U. S. forces have deployed on station to initiate casualty-producing actions. At this point, withdrawal may be considered more dangerous than continued engagement. This was one of the factors that delayed the ultimate U. S. pullout from Vietnam.

The strategy should also deny the U. S. any visions of a quick victory, and if possible, of any sort of victory. Early in the conflict, any casualty-producing engagement between U. S. and NPC forces should result in an overwhelming NPC victory. This will serve to deny the American public any vision of ultimate victory. It will make the mere fact of casualties more devastating than their actual numbers dictate and will diminish America's willingness to accept future casualties. The early engagements must therefore be carefully planned and replanned, allowing for any and all contingencies. Sufficient forces must be allocated to guarantee success. Follow-on actions and contingency actions must also be planned for success. America must not be given any sign that it can be victorious during the early stages of the war. They cannot be allowed to conduct the equivalent of Jimmy Doolittle's bombing of Tokyo (on 18 April 1942) only four months after Pearl Harbor [124]. America cannot be allowed to follow its battle plan unchallenged. The equivalent of the lengthy and orderly buildup of Coalition forces prior to Desert Storm cannot be allowed to proceed successfully. A successful Iraqi capture and occupation of Khafji (instead of the unmitigated disaster it turned into) followed up by additional successes might have altered the outcome of the Gulf War [125], [126].

However, NPC must make every effort to avoid too much surprise. The U. S. will react to another Pearl Harbor with just as much moral indignation and desire for vengeance as it did fifty-eight years ago. When NPC decides to initiate the hostilities (it can be reasonably assumed that NPC will be the aggressor), it must pay careful attention that the United States Government and its people know in advance that those hostilities are imminent. Tactical surprise can be maintained, but the potential for a declaration of war, and the specific actions which will bring such a declaration into being need to be communicated in advance, in clear and simple language.

Actions should be taken ahead of time to call the motives of the U. S. Government into question with regard to the topics of potential NPC-U.S. conflict. NPC should try to justify that it has the moral high ground in any conflict. It should take any action within its power (that does not violate NPC fundamental policies) to reinforce its supposed moral superiority. Any instance of American moral turpitude that can be found (or manufactured) to degrade America's claim to the moral high ground should be paraded before the United Nations and the world press.

The U. S. Government should make every effort to ensure that its military forces are placed in harm's way only when vital national interests are involved. In such situations the civilian population is somewhat more tolerant of casualties, although excess is deplorable no matter how important the cause. However, the author recognizes that society does not always engage only in "righteous wars", such as World War II, and occasionally situations will arise in which military forces are employed without full support of the general public. In such situations, the U. S. military should recognize that adversaries might attempt to use massive casualties as a strategic weapon. Forces should never be sent into a crisis or conflict situation without consideration that the adversary might be planning a trap or pre-emptive strike against those forces (with the adversary's primary goal being the infliction of unacceptable levels of casualties). Some adversaries might even be willing to suffer greater losses or cede tactical advantages to the U. S., if the level of U. S. casualties ultimately gives them a strategic advantage. The 1968 Tet Offensive was a tactical defeat of catastrophic proportions for both the Viet Cong and the North Vietnamese Army, yet it so turned the tide of public opinion in the United States that it was a strategic victory. Pre-mission intelligence gathering should pay attention to this possibility and attempt to ascertain to what ends any adversary is willing to go.

RESTRICTIVE RULES OF ENGAGEMENT

A rule of engagement is an order from higher command to subordinate warfighters outlining what targets may be engaged, under what conditions they may be engaged, and with what degree of force they may be engaged. "Don't fire until you see the whites of their eyes" is a rule of engagement. The United States is very solidly in favor of maintaining the moral high ground and obeying the rule of law. As seen in the previous section the American military also strongly wishes to avoid fratricide. Since the U. S. military is an instrument of U. S. foreign policy, that policy also imposes limits on what we can or cannot do. Thus, military commanders issue rules of engagement that attempt to keep the moral high ground, obey the Laws of War [127], satisfy foreign policy objectives, and minimize fratricide.

To keep the moral high ground we generally:

- ***Avoid bombing or shelling residential areas of cities (although in World War II and Korea, we did not always follow this rule – as the residents of Hamburg and Dresden could attest [128].***
- ***Avoid bombing or shelling sites of great cultural, religious, historical, or archaeological interest.***
- ***Avoid bombing or shelling schools and hospitals even when the enemy uses those facilities for key military purposes (many North Vietnamese hospitals had air defense weapons mounted on their roofs or sited in their courtyards).***
- ***Avoid bombing or attacking civilian air raid shelters if these can be identified***
- ***Avoid shooting or otherwise injuring unarmed civilians.***
- ***Avoid attacking passenger aircraft and ships.***
- ***Avoid attacking any commercial craft without verifying its registry.***
- ***Avoid destroying key facilities (such as dams or nuclear reactors) whose destruction would have catastrophic effects on the civilian population.***

In the realm of foreign policy, we may opt to:

- ***Avoid firing the first shot, unless unequivocal intention that a threat intends to attack U. S. assets can be determined.***
- ***Avoid any military action that might upset a Coalition member or a "neutral" country (In the Gulf War we prevented Israel from participating to foster the Coalition with the Arab states; In Korea and Vietnam we refrained from using nuclear weapons to avoid a possible nuclear confrontation with the Soviet Union)***
- ***Conduct a military action with a minimum of forces or a minimum level of force to avoid the appearance of "beating up" a weaker opponent.***
- ***Respect the wishes and national sovereignty of non-participant states (such as not overflying their territory with military aircraft during deployments or strike missions).***

To minimize fratricide or accidental losses, we may:

- ***Avoid firing on any target we cannot positively identify as hostile (this often translates to requiring visual identification of the target, and precludes the use of long range standoff weapons at their maximum ranges).***

- ***Avoid firing at hostile targets that are in close proximity to friendly forces.***
- ***Require friendly forces to carry devices or markings that aid in their positive identification (such as the black and white stripes on the wings of Allied aircraft participating in the Normandy invasion).***
- ***Prohibit flight training at minimum altitudes (even though those minimum altitudes will be violated in combat).***

To obey the Laws of War, we will (among other things):

- ***Treat prisoners of war in accordance with the Geneva Convention.***
- ***Avoid the use of torture during interrogation.***
- ***Avoid the use of excessive force.***
- ***Avoid the use of chemical and biological weapons.***
- ***Observe the rights of neutral states.***
- ***Avoid looting or pillaging of occupied territories.***
- ***Observe the civil rights of civilians in occupied territories.***
- ***Avoid unnecessary destruction of private property in occupied territories***

The restrictive nature of a rule of engagement may increase the vulnerability of U. S. forces. For example, a policy of "don't fire the first shot" will lead to casualties in situations where "he who fires first, wins" as was often the case in armored combat (the lethality of tank weapons exceeded the protective capabilities of their armor). The policy of requiring positive visual identification of an air target before firing totally negates the benefits of having long-range missiles such as Phoenix or AMRAAM. Observing no-overflight requests from a nation may force a strike force to fly hundreds of miles farther and subject itself to earlier detection when performing a strike mission. The extra pilot fatigue, increased opportunity for component failures, and advance warning to the enemy may easily result in increased casualties.

The author recognizes that many rules of engagement must be followed. Nevertheless, this does not alter the fact that they may increase the vulnerability of our forces. Unnecessary rules of engagement should be avoided. It is possible for the enemy to exploit vulnerabilities created by those rules of engagement.

NPC should make every effort to understand the rules of engagement under which the U. S. forces will operate. It should take every opportunity to exploit any vulnerability that those rules may create. If NPC places a lower value on human life than the U. S. then it should exploit our dislike of producing civilian casualties. They should co-locate critical military facilities such as command, control, communications, intelligence, and surveillance facilities with schools, churches, hospitals, orphanages, playgrounds, or day-care facilities. Even better, they should bury their critical military facilities underneath such civilian facilities. Air defense sites should be located on top of such facilities. Barracks and military housing might be fully integrated into civilian housing areas ringing military facilities.

NPC may wish to consider staging events that will cause tightening of the rules of engagement. For example, it might recreate a "*Vincennes* incident", in which a U. S. warship might shoot down a civilian airliner [129]. This might be done by having a stealth platform fly above and behind a civilian airliner on a flight path that would carry the airliner directly over the warship. By replying with military IFF codes when the airliner was interrogated by the warship and transmitting messages to ground control on military frequencies, the stealth platform would give a false identity to the airliner. Sensors on board the warship would be unable to detect the stealth platform and would see no azimuth or elevation angle difference between the radar return from the airliner and the signals picked up by the ESM and the IFF systems. At an appropriate range, the stealth platform could first radiate search radar signals, then tracking radar signals, and finally missile guidance signals. The U. S. warship might justifiably believe it was under attack and retaliate by shooting down the obvious source of the threat (the airliner). NPC would have to be willing to sacrifice civilian lives for military purposes, but many potential adversaries have demonstrated just such willingness. If unwilling to do so, it would not be difficult for NPC to outfit the airliner to be remotely piloted.

With appropriate cunning, planning, and preparation it should not be difficult for NPC to stage one or more incidents of "fratricide". Captured U. S. units might be covertly relocated to areas near the front, which are almost certain targets for artillery or air strikes. With widespread tactical communications jamming, it is almost a certainty that some units will become "lost" to the command and control network. If such units suddenly where no friendlies are supposed to be and known hostiles are expected to be, they will be attacked without much hesitation (the first time). After a quick policing of the site after the attack to guarantee a lack of survivors who could tell what really happened, U. S. forces which later captured the site could only report their discovery as an example of friendly fire. Similar incidents involving units from different allied nations might be used to spread distrust among Coalition members. NPC might also commit atrocities (a la the My Lai massacre) using special operations forces wearing U. S. uniforms, carrying U. S. equipment, and speaking English. The results of multiple events such as those described above would likely be a severe tightening of several rules of engagement. The tightening will almost always cause delays in responding to an attack or in pressing home an attack that are advantageous to the adversary.

No professional military force can operate without rules of engagement. Most of those imposed are well justified by the political situation and by international law. However, senior commanders (including the President) have a duty not to make the rules of engagement overly restrictive. Furthermore, they need to be aware that a clever adversary might try to exploit those rules to his own advantage.

One action that can be done by U. S. forces prior to the exploitation is planning. This planning is essential to minimize the advantage that an adversary might gain. It should include reactive and retaliatory response options. Forces and equipment necessary to effect those options must be kept unallocated to other tasks. Should an event occur that threatens to cause tighter rules of engagement to be imposed, that event should be thoroughly researched and dissected to guarantee that the event was not staged deliberately to provoke an overreaction.

The U. S. also needs to develop weapons and equipment that can relax the rules of engagement. Improved warning systems are one such development. The *earlier a potential threat can be detected and the more attention that can be devoted to assessing whether the potential threat is an actual threat or not, the less restricted are the engagement options when the time for engagement actually arrives. The warning system might also provide improved information needed to correct a bad situation. For example, a bullet-tracking sensor might detect a single shot from a sniper and indicate the window from which the bullet was fired. An immediate response would probably catch the sniper red-handed. Without the sensor, the alternatives include: leaving the area and sacrificing the mission, returning massive amounts of unaimed fire for each sniper shot (and possibly injuring many innocent people), or possibly suffering days of sniper attacks leading to excessive nervousness and irritability on the part of the troops that might flare into a subsequent war crime (such as My Lai).*

Effective nonlethal weapons are another potential development. If an individual (hostile or otherwise) can be soundly deterred from closing to threatening ranges, questionable situations might never arise. Should a questionable situation arise, then the ability to "shoot them all" without having to let "God sort the good from the bad afterwards" allows for defensive actions to be taken that cannot have potentially unacceptable repercussions. With nonlethal weapons available, then the U. S. forces could shoot first in a threatening situation, but would not have the potential drawback of dead or wounded noncombatants or innocent bystanders. If a small boat appeared to threaten a U. S. warship by attempting to get too close, then a nonlethal weapon might incapacitate that small boat at a safe distance, allowing a more thorough investigation of the circumstances before more final actions are taken.

CIVILIAN INTOLERANCE OF UNNECESSARY HARDSHIPS

Americans are willing to tolerate almost anything as long as it does not affect them directly. However, when an action directly limits the lifestyle or behavior of an individual, that individual is resentful, unless he can be convinced that the limitation is necessary. If a conflict can be conducted with little or no impact on the average American, that average American will probably not pay much attention (beyond that imposed on him by the media). If on the other hand, that average American's ability to pursue life, liberty, and happiness is limited because of a conflict, the average American will demand reasons that such limitation is necessary. Fear for the safety of self or family is one of the strongest of such reasons.

Past conflicts have imposed a variety of hardships or lifestyle limitations on the American public. Until the 1970's American youth was subject to the "draft", the Selective Service System. A lottery was used to provide enlisted personnel for the armed forces. Although deferments could usually be obtained for college education and employment in critical fields (such as defense technology), the draft meant a potential for a young person's life to be diverted from his planned course for several years. In the 40's, 50's, and 60's, this diversion was accepted because the fear of attack by real enemies (Germany and Japan in the early 40's and the Soviet Union in the succeeding 25 years). By 1970, the fight against Communism in Vietnam was viewed as unnecessary by so many youth that draft cards were burned at public rallies and more than a few that were drafted fled to Canada to avoid service. The move to volunteer armed forces eliminated the Draft (although in the 1990's the unattractiveness of a military career may force its reinstatement).

In World War II there was food and gas rationing. The righteousness of WW II made these hardships tolerable. When a "political conflict" led to the Arab Oil Embargo in 1973 with its long lines at gas pumps and restricted purchase of gasoline on alternate days. The inconvenience was significant (increased prices and hours wasted by everyone with an automobile) but the threat was low. There was local violence and serious questions thrown at government representatives. Many people believed that the gasoline shortages were orchestrated by the oil companies to raise prices. The Gulf War led to heightened "security" at airports and delays in boarding flights. The public was inconvenienced, but not excessively. Most people accepted the inconvenience because they were afraid of the terrorist acts of violence that Saddam Hussein had promised.

If the U. S. enters a major conflict with a near peer competitor, there will be hardships imposed on American citizens. The call-up of reserve forces will inflict financial hardship on many families (the civilian jobs of many reservists pay 2-3 times what the reservists earn on active duty). Airport security will be further heightened. If the buildup of forces abroad requires exercising the CRAF option on a large scale, then the resulting shortage of passenger aircraft will require many business and pleasure travelers to forego their travel. If the conflict is high-intensity and lasts for more than a month, our reserves of fuel oil and gasoline may be sufficiently depleted that gasoline rationing may need to be instituted. The threat of terrorist violence may cause a declaration of a state of emergency with the imposition of martial law.

The American public may or may not tolerate these hardships. If the CRAF option prevents families from going home for Christmas or puts some firms out of business because their employees cannot travel or their products cannot be delivered in a timely fashion, then the U. S. government had better have done a good job of convincing the public that the conflict and the hardship actions are necessary for national survival. Protecting the sovereignty of some small nation with no vital resources and limited market for trade may not be sufficient justification. The same is true of gasoline rationing. If the threat of terrorist action forces the imposition of martial law, that threat had better openly manifest itself and directly threaten the wellbeing of the general public. If it only threatens the military, many citizens will not be willing to tolerate frequent police challenges, curfews, travel restrictions, and searches and seizures. In fact, the "unjustified" imposition of such measures may provoke a "militia" backlash far more destructive than the original terrorist threat.

In short, the American public will tolerate any hardship if they are convinced of its necessity or if they are fearful for life or property. If they are not fearful for life or property and they have not been convinced of the necessity of a hardship, they will not tolerate that hardship for long. They will blame the Government that imposed that hardship, not some faceless overseas adversary. They will either remove their elected representatives at the next election or they will openly violate the restrictions.

NPC should attempt to create situations in which the U. S. will impose hardships on its own citizens. They must take care not to directly threaten the civilian population when they create those situations. NPC special operations forces might conduct a series of "terrorist" attacks on government and military equipment and facilities around the United States. Military casualties should be minimized and civilian casualties should be scrupulously avoided. The end goal would be the imposition of martial law in the United States proper. Deliberate attacks on a few senior governmental and military officials might be the most effective at provoking this response without provoking significant fear in the general public.

NPC could also attempt to disrupt those sectors of the American economy that impact the most members of the American public. For example, NPC could disrupt air travel by forcing the CRAF to be drafted for military use or by infecting the air traffic control system with a virus. NPC could curtail automobile travel by arranging for temporary shortages of oil and gasoline supplies. By staging accidents (fires or explosions) at a number of oil refineries during the month or two preceding any hostilities and by outbidding competitors for crude oil supplies on the spot market during the same period, NPC could arrange for a temporary shortage of refined fuels in North America. By itself this might only cause increases in gasoline, diesel, and heating oil prices. But coupled with the U. S. Government exercising priority over the fuel supplies to support the massive sealift and airlift requirements associated with power projection, serious civilian automotive fuel shortages would arise. Gas lines would become regular occurrences and rationing might become necessary. If the conflict occurs in the late fall, winter, or early spring, then many citizens in colder part of the country will suffer from shortages of heating fuel. Other inconveniences that might be inflicted on the public include shortages of meat, milk, or other specialty foods, shutdown of cellular telephone traffic, and loss of key television services.

The U. S. Government should make every effort to ensure that its military forces are placed in harm's way only when vital national interests are involved. In such situations the civilian population is somewhat more tolerant of inconveniences. In situations in which military forces are employed without full support of the general public, the U. S. military should recognize that adversaries might attempt to use civilian disruption and inconvenience as a strategic weapon. If military actions such as calling up the Civil Reserve Air Fleet appear to be necessary, the likelihood that this might be part of an adversary's strategy should be included in the deliberations and planning.

Homeland Defense studies should focus part of their activities on this topic. The full spectrum of possible "disruption and inconvenience" activities should be identified. A few are described above, but there are many more. For every "inconvenience" identified, prevention strategies, defensive measures, and remediation responses should be developed. If new research and development initiatives are required, they should be incorporated into the funding priorities of the appropriate development agencies.

NEED FOR COALITION SUPPORT

In the past decade the United States has shown an increasing tendency to require international agreement on, international cooperation with, and often direct international participation in its foreign military operations. Many (if not most) Americans do not believe that we can afford (either financially or politically) to act unilaterally. The progressive reduction in U. S. overseas presence manifested by the closure of some U. S. overseas military bases and the loss of other permanent bases due to changes in host country politics will also cause increased needs for international cooperation.

Many factors can affect whether or not that cooperation or participation is received. In the case of joint participation in military operations, it is important to establish that our allies national interests are at stake not just those of the United States. Potential adversaries can use propaganda, disinformation, economic or other political negotiations (offering highly desirable incentives or seriously punitive sanctions), extortion, or even threats of military action to adversely influence the perceptions of our allies. In the case of use of overseas bases, the host country must decide that cooperation with the U. S. will not harm it in the long run. Their perception of U. S. intentions in using these bases must be consistent with their own resulting long-term benefit. However, the perception of true U. S. intentions can be influenced by propaganda from potential adversaries or their allies. A potential adversary can apply or support both external and internal threats to the integrity of a host government. These will almost always affect the host's willingness to cooperate. Economic relations and standing political alliances are other significant factors.

Through any or all of these means, an adversary might prevent the United States from getting access to foreign port facilities or airfields. It might cause withholding of rights of passage through foreign territorial waters or overflight by U. S. forces. It might cause decreased "coalition" commitment of troops, monetary support, or logistics support. It might even enlist open military action against U. S. forces by a former neutral or weak supporter. Any of these actions will cause significant alteration in the way the U. S. has planned to conduct the military operations. They will also reduce the effectiveness of U. S. forces in conducting those military operations and may increase both the monetary costs and the casualty costs of those operations.

NPC should make every effort to establish friendly political and strong economic relationships with all of the countries that might be of military use to the United States. Some of these relationships may be based on substantial, but covert bribery of key government officials. Using any and all of these relationships, pressure should be continually exerted on these other countries to reduce their political and economic ties to the United States. In time of hostilities, NPC should be willing to adversely terminate any or all of the relationships with any country that sides with the U. S. An attempt should be made to establish a regional defense alliance (excluding the United States) with all of those same countries that belong to the region of interest. NPC should use this regional alliance to attempt to resolve any and all disputes. By judiciously pursuing (and occasionally losing a few unimportant) claims before this alliance, NPC can establish a precedent for excluding the U. S. from deliberations. This will weaken any support the U. S. might expect from the United Nations.

Every attempt should be made to establish or at least portray the United States as the aggressor in any confrontation with NPC. Such attempts might include strategic deceptions and disinformation campaigns orchestrated to provide alternative explanations for any hostile NPC move. These deceptions should be maintained over time despite any transparency that may occur. Effective and visible threats should be developed that can be held over any country of military use to the United States that does not accept close political and economic ties with NPC. These threats might be military or economic in nature. They should be orchestrated well in advance, so that both NPC and the threatened country are fully aware of their existence, and of NPC seriousness in carrying them out.

Although coalition warfare is preferable from public opinion and cost perspectives, the requirement for a coalition creates a vulnerability. The U. S. military should be capable of unilateral action wherever and whenever necessary. It should not be deficient in critical capabilities (such as mine warfare) that absolutely require cooperation and participation of one or more key allies to alleviate. In the event of a "righteous" World War III, where coalition warfare will be essential to national survival, the needed coalition will form naturally, a la NATO, and be reasonably robust. In lesser crises and conflicts, coalition warfare should never be a requirement, only a desired mode of operation. With respect to actions designed to weaken a coalition, the U. S. should anticipate them wherever possible, and take counteractions, if reasonable. For example, if an adversary is holding a coalition partner hostage to ballistic missile attacks, the U. S. needs to be prepared to supply ballistic missile defense (whether complete forces or only required items of equipment) to that partner. The U. S. should discourage potential coalition partners from entering into alliances with potential adversaries.

UNEQUAL SOCIETAL TRANSPARENCY

The United States is a remarkably open society whose actions are usually transparent to all outside observers. This openness is one the major strengths of American democracy. It also has a flip side in that it is relatively easy to determine what actions the United States is taking and why. We have few true secrets and are relatively predictable in our responses to external stimuli. Societal complexity prohibits an enemy from perfectly predicting our actions, but the observant enemy will be right more often than he is wrong. In peacetime we are willing to share virtually all knowledge including military knowledge (but excluding truly classified information) with almost anyone who is not an actively avowed enemy. Military students from dozens of foreign countries study at our military academies and war colleges. They learn the doctrine and tactics that the U. S. will use should it go to war. They make friends with their American officer peers and learn how these future military leaders think. More senior allied officers often serve exchange tours with U. S. units. They participate in operations and in exchange offer insights and analyses of how those operations might work in a coalition warfighting effort. Other officers routinely serve as military attaches in their embassies in Washington. Although the U. S. sends its share of officers to serve with other militaries in these exchange programs and possesses its own cadre of military attaches overseas, we do not send our junior officers to study at foreign military academies. Their careers are too filled with required tours of duty to "waste" any time studying overseas.

Civilian students from virtually every country in the world attend major U. S. universities. Here they study all aspects of our culture, society, government, industry, and especially our technology. Foreign workers are accepted to work in almost every major industry, with limited exceptions at defense contractors. In some critical areas in the electronics and software industries we actively recruit these foreign workers. We know little about how many of these are actively aiding the intelligence agencies (or perhaps the industrial organizations) of their home countries. To gain the economic benefits of increased foreign trade, U. S. companies are willing to enter into co-production agreements that serve to transfer critical technologies and intellectual capital to the foreign firms. When these technologies are dual-use, the foreign firms show little reluctance (despite any agreements to the contrary) to adapt the newly acquired American technology to improve their own military forces.

Although the interactions with foreign students, civilian workers, military officers, and government officials do act to strengthen the United States, the transfer of knowledge clearly helps our adversaries as well. It is likely that more knowledge and information are exported than imported. This is a vulnerability that we cannot eliminate. We need to avoid the isolationism of the past. Our economy is too deeply involved with those of other countries. However, we should be aware of the problem of unequal societal transparency and attempt to eliminate one-sidedness whenever possible.

NPC should make maximum use of the transparency of U. S. society. A large fraction of NPC's university students should be encouraged and subsidized to study at U. S. universities. These students should be further encouraged to study vital technologies and any aspects of U. S. society, culture, and government that would aid in predicting U. S. policies and responses. Some of these "students" should be drawn from the intelligence community. These will be allowed to remain in the United States after their formal education is completed. They will act to insure that NPC is kept abreast of all major technology and cultural developments occurring in the U. S. Students not willing to work in intelligence capacities after graduation should be strongly encouraged to return to NPC to work in the growing scientific and industrial complexes being developed.

NPC military officers should be encouraged and subsidized to attend advanced military schools (such as the Air University, War College, Naval War College, and Naval Postgraduate School). The officer students should learn to read, write, and speak English. They should befriend their American counterparts, and where possible they should maintain some sort of contact after they return to NPC. This not only facilitates access to information but also its flow. It also establishes a number of back channels for communication that may prove useful in times of crisis.

Every attempt should be made for select units to be posted to the U. S. to undergo joint training or exercises. Exchange programs involving individual officers should be instituted. Of course, the reciprocal exchanges will not be on a true parity basis (although they will be described as such in all communications) in order to ensure that the flow of information is as close to one way as possible. A senior NPC naval officer might be assigned to a Fleet command, but his U. S. counterpart might be stationed at a military shipyard or a logistics depot.

NPC companies should establish cooperative development programs with U. S. companies to effect one-way transfers of critical technologies or to build up industries and industrial capabilities of strategic importance to NPC. Dual use technologies should be emphasized in these programs although the military aspects should be avoided in all external communications. These programs should be subsidized to make sure that they are profitable to the U. S. companies (at least in the short term) so that those U. S. companies are eager to repeat the process and join in even more technology-transferring ventures. Products that NPC companies have developed should be actively exported to gain foreign exchange credit, but technologies and inventions that permitted the development of those products should not be transferred unless dual use can be ruled out.

The United States is a democracy that has retained that status because it maintains a high degree of societal transparency. The U. S. should not take any actions that severely reduce its own transparency. This does not imply that we should pay less attention to espionage and intelligence operations on the part of any adversary. Counterintelligence should be a high priority. Fewer foreign nationals should be allowed access to critical facilities such as military bases and national laboratories. U. S. corporations should be encouraged to employ U. S. citizens in sensitive high technology positions, rather than rely on importing foreign scientists and engineers, who will work for lower pay.

The U. S. should consider taking a number of actions to increase the transparency of potential adversaries. On-site inspections should be a mandatory part of *any arms control agreement. When U. S. dignitaries visit foreign facilities, if they are given meaningless tours, then dignitaries from that country should be given equally meaningless tours and make it known that such treatment is tit-for-tat. For example, if the U. S. Secretary of Defense visits a country and asks to visit his counterpart's headquarters, and instead is met in the office of a trade delegation, then when that counterpart visits the United States, he should be received in the office of a District of Columbia bank, rather than in the Pentagon. If an officer exchange program is established, then the quality of assignments given to the foreign exchange officers should match the quality of assignment given to their U. S. counterparts. Human rights, especially freedom of speech, freedom of the press, and freedom of movement should remain key aspects of any and all economic negotiations with potential adversaries. Favored treatment should be withheld until noticeable improvement in transparency occurs.*

TREATY LIMITATIONS

The United States is party to numerous treaties that place limits on allowable military actions and equipments. See Appendix L for a comprehensive examination of arms control treaties, their signatories, and the limitations they impose. ***The United States is known for the fact that it honors its treaty obligations. Some potential adversaries are not parties to critical treaties. Other potential adversaries have histories of less than strict compliance with provisions of the treaties they have signed. Any treaty with militarily-limiting provisions to which the United States is a signatory, but to which any potential adversary is either not a signatory or whose provisions it ignores, creates an asymmetric military situation in which the United States is at a distinct disadvantage.***

For example, if the United States ratifies the Comprehensive Test Ban Treaty (CTBT), it will be unable to test the reliability of any of its existing nuclear warheads. Since warhead production facilities have already been shut down as a consequence of warhead reductions required by the START treaties, new warheads (of old designs) cannot be assembled to replace aging warheads. As a result, the ability of the United States to rely on its nuclear arsenal to work as designed will diminish with each passing year. At some point, the United States will have no confidence in its nuclear arsenal and it will be more of a liability than a deterrent. If any nuclear power fails to ratify and abide by the CTBT, then it will be able to test its existing weapons as well as to develop improved warhead designs. Such concerns are one reason the U. S. Senate has refused to advise the President to ratify the CTBT.

If any nuclear power clandestinely decides to violate the Outer Space Treaty and place nuclear warheads on orbiting platforms, the United States could be subjected to decapitating nuclear strikes with at most a few minutes warning (and possibly no warning). Evacuation of National Command Authority and other major Government elements to secure locations or shelters would probably not be possible. It is also possible (although unlikely) that we would be unable to attribute the strike to any particular adversary. Given that it was debatable that a reasoned response could be developed even with the 30-minute warning to which we were accustomed during most of the Cold War, it is almost certain that no response would be forthcoming from the highest command levels before they ceased to exist.

Many treaties might be exploited in some way to provide a military advantage to a potential adversary. Foremost among these include the following:

- ***Non-Proliferation Treaty***
- ***Chemical Weapons Convention***
- ***Biological & Toxin Weapons Convention***
- ***Outer Space Treaty***
- ***Antarctic Treaty***
- ***Seabed Treaty***
- ***The Test Ban Treaties***
- ***The Nuclear-Weapon-Free Zone Agreements***
- ***The SALT and START Treaties***
- ***Intermediate Nuclear Forces Treaty***

- ***ABM Treaty***
- ***Open Skies Treaty***
- ***Nuclear Material Treaty***
- ***Fissile Material Production Cut-off Treaty***

The contents and characteristics of these treaties are summarized in Appendix L.

NPC should attempt to create asymmetric military situations advantageous to itself either by selective non-compliance with treaties to which the United States is a State Party or through failure to sign and ratify treaties that the United States is likely to ratify. However, any non-compliance must be done selectively, and to the extent possible, done clandestinely. Secrecy or at least discretion is required because blatant non-compliance will focus U. S. attention on NPC and its possible future actions. This may result in U. S. development of counters to the NPC actions and possibly military intervention to preempt any situation that the U. S. feels has become untenable.

Failure to ratify a treaty should only be pursued after careful weighing of the military advantages that might accrue against any disadvantages that might accrue. in the form of economic sanctions or political "ill will". The intent is to establish a net advantage relative to the U. S. However, this advantage must consider factors beyond military power. Failure to ratify a treaty might result in economic sanctions. For example, failure by NPC to ratify the Non-Proliferation Treaty (NPT) and negotiate an IAEA Safeguards agreement would prohibit NPC from obtaining fissionable material in any form from any country that had signed the NPT. Failure to ratify might also create increased ill will between NPC and potential adversaries, quite likely including the United States. Those adversaries might respond by increasing their military preparedness, leaving NPC at a net disadvantage. The response might take the form of strengthening alliances between several potential adversaries to NPC, also producing a net disadvantage.

The United States must take a leadership role in international politics. As a consequence, it cannot avoid entering into treaties and other arrangements that limit its military power or options. Most of the treaties that are ratified by our Government provide net benefits to the United States. Nevertheless, they provide opportunities to ruthless or dishonorable adversaries. We need to find ways to limit those opportunities without either reneging on our agreements or failing to participate in international negotiations. It is important that any treaty to which the U. S. becomes a party must include viable provisions for compliance verification and serious, enforceable penalties for failure to comply or violation of any treaty provision. The treaty must not contain loopholes or language subject to misinterpretation that would permit one party to engage in preparations towards a treaty violation without sanctions being enforced. Wherever possible, prohibitions should be absolute to minimize loopholes. For example, a treaty should not ban long-range missiles without banning short-range missiles as well. Short-range missiles are too easily converted into longer-range missiles by simple improvements in technology that are difficult to detect via verification procedures.

The United States should review the major militarily-limiting treaties to which it is a party and evaluate the ratification status and compliance histories of potential adversaries with respect to those treaties. It should determine what benefits could accrue to those adversaries should they fail to fully comply with treaty provisions. The U. S. should examine plans to counter those accrued benefits. The counters might include developing new tactics, changing existing force structures, altering planned deployments of those forces, hardening existing military equipment and facilities, or developing new equipment and facilities. The U. S. should also task its intelligence apparatus to improve its monitoring and compliance verification activities related to those treaties and those potential adversaries.

During future treaty negotiations (before the treaties are signed), the U. S. military should evaluate the effects of proposed treaty limitations. It should assess the likelihood that one or more potential adversaries will exploit those limitations, determine the manner in which exploitation is likely to manifest itself, and make contingency plans to develop counters to the exploitation. This assessment should be made available to the Cabinet, the treaty negotiators, and Congress prior to critical decisions/concessions being made.

CHAPTER X. TECHNOLOGICAL CHANGE

TECHNOLOGICAL SURPRISE

The world is becoming more technologically complex with each passing day. The technological half-life of the average technology is roughly 15 years. In some fields it is two years or less. In one technological half-life, a body of new knowledge, new techniques, new theories, new inventions, etc., is "created" that is as large as all of the knowledge, etc., that has been discovered in all of prior history. For every major field of endeavor, after one technological half-life there is likely to be a second uniquely different major field of endeavor. Consider the roughly sixty-year period since the start of World War II. At the start of this period (1939) UHF/VHF radar had become a practical tool (the CHAIN HOME system). A few years later (1943-45) it had been replaced by microwave radar in the majority of applications. Perhaps a decade later (circa 1955), the foundations of synthetic aperture radar had been established. Another decade later (circa 1965) laser rangefinders had come into practical use. After yet another decade or so had passed (circa 1975), serious work on over-the-horizon radars had started. By the mid-1980's true radars operating at laser wavelengths were searching for deployable applications. Finally, at the end of the century, netted multistatic radars were beginning to be considered as serious contenders for counterstealth applications. Each of these inventions, occurring roughly once a decade, opened military possibilities undreamed of previously.

Given the rapid rate of technological change, any country is open to technological surprise. No country can afford to give priority funding to every possible technology. It doesn't matter whether the funding comes from commercial or government sources, some technology areas will not be adequately funded. However, many other countries look for niches that they can occupy and compete with the industrial giants. A technology area that one country fails to diligently pursue is likely to be pursued by a competitor. If an adversary country invests in an area that produces a militarily significant breakthrough and can keep it secret (or at least make it appear unimportant) during development and deployment, then that adversary has a significant window of relative superiority that it can exploit. It may even be the equivalent of a "technological Pearl Harbor". If the U. S. has not kept pace technologically, it will take a substantial passage of time to close that window of vulnerability.

It is considerably more difficult to effect a significant degree of technological surprise, if both sides have roughly comparable levels of expertise in a subject. In addition, the duration of any window of vulnerability will certainly be shorter, if the surprised party is only a short way behind the surprising party in the relevant technology. The U. S. will become more vulnerable to technological surprise as it relinquishes it leadership in more and more technologies (a trend that also creates a second distinct form of vulnerability in the form of technological atrophy).

NPC should attempt to achieve technological surprise over the United States and/or other adversaries whenever possible. It should invest heavily in research and development activities in many fields. Such investment will serve three purposes. First, it will provide incentives for NPC's youth to enter scientific and technological fields of endeavor. Second, it will provide a plethora of new discoveries that will fuel NPC's economic development in the same way that the U.S.'s leadership in research in the 60's, 70's, and 80's kept the U. S. economy dominant in a world market. Third, it will provide opportunities for technological surprise. How much investment should NPC make? The author believes that it should be as much as the economy will tolerate. It is one form of "arms race" that one cannot lose by spending too much. Every dollar invested in research will do nothing but aid the economy in the long run. NPC can only ensure opportunities for technological surprise if it is willing to outspend the U. S. in research and development.

Despite this, NPC should exert some form of strategic control over its research and development activities. Strength against strength is seldom a good military practice. NPC should not try to outspend the U. S. in those areas in which the U. S. has a clear lead. It cannot ignore those areas, but it should spend only enough to be able to respond quickly to critical U. S. developments. Instead, NPC should identify those technology areas where the U. S. is weak and devote the lion's share of resources to funding those technologies.

NPC should attempt to control the flow of information from its research and development activities. This is a tricky process. Enough information must flow out to insure that NPC is taken seriously as an R&D state. This information will aid in the sale of products on the international market and aid in the penetration of foreign R&D activities. However, technological surprise is not possible if all information is freely shared. Critical results must be hidden or at least delayed. This must be done without altering the apparent external flow of information. When researchers suddenly stop publishing on a subject, it is an immediate cue to an aware intelligence organization that one of two things has happened: the group has stopped publishing because a researcher has died, his funding has been cut off, or his group has been disbanded; <u>or</u> the research has suddenly become classified.

The United States should revise its research and development strategy in order to minimize the prospects of technological surprise. No country today can be the leader in every field of technology development. However, it is important to be a credible player in every field. Failure to do so can lead to technological surprise. The actions that the U. S. should take to prevent technological surprise are essentially the same as those needed to avoid technological atrophy. We will discuss them at the end of the next section.

TECHNOLOGICAL ATROPHY

During much of the 20th Century the United States has been a leader in the development of advanced technology. However, it has not always been so and there is reason to worry that it may not remain true much longer. A smaller percentage of the population is being educated in technological fields. Few high school students take more than one science course or three math courses. Few take advanced placement courses in math or sciences. Thirty years ago, it was common for any "college prep" student to take at least three years of science and four years of math. Every school had a dozen or more students taking one or more advanced placement courses. High schools often have teachers teaching math and science classes who did not themselves major in or even specialize in math or science. Teams from the United States regularly fail to place anywhere in the top 10 in international high-school level science and math competitions. Scores on graduate record examinations for U. S. students have fallen during the last decades of the 20th Century.

Today, science, engineering, mathematics, and computer science/programming courses represent a smaller fraction of the total number of courses taught at a typical college than in past decades. Although most college graduates are highly computer-literate, few are technology-oriented. They use computers as tools for business or other purposes, but do not know how computers are built or software is generated. Roughly half of all graduate students in science and engineering at U. S. universities come from foreign countries and the percentage is rising. Although the number of U. S. citizens pursuing college educations is increasing and expected to soar in the next decade, total enrollments in science and engineering graduate programs are still decreasing. This decrease is occurring in spite of increased foreign student enrollments. The total number of engineering degrees granted in the U. S. declined 17.8% from 1986 to 1996. The number of computer science/mathematics degrees awarded declined 35.8% over that same period. During the period 1975 to 1997, the fraction of the 24-year-old population with degrees in science and engineering in the U. S. rose 35% from 0.04 to 0.054. However, in most industrialized countries, the percentage increase ranged from 50% to as high as 450%. In Britain, the fraction rose from 0.029 to 0.094; in South Korea, the fraction rose from 0.020 to 0.090; in Germany, the fraction rose from 0.033 to 0.081; in Japan (our biggest technological rival), the fraction rose from 0.047 to 0.072; in Taiwan, the fraction rose from 0.026 to 0.068; and even in mostly agricultural China, the fraction doubled from 0.004 to 0.008. [236]

Every year, businesses in Silicon Valley and elsewhere plead for visa for hundreds of thousands of foreign scientists/engineers/programmers. There are not enough U. S. citizens or immigrants with permanent resident visas with the desired skills to fill the personnel requirements of those businesses. There is also no sign that the U. S. is taking adequate steps to produce an adequate number of educated residents to fill the open positions.

In the 50's and 60's there was active governmental interest in increasing enrollments and interest in science and technology. The Space Race and the Cold War were both at their heights. Most of the author's older scientific and engineering acquaintances, almost all of whom grew up during this period had science or mechanics as a hobby. Many had chemistry

sets or access to chemistry laboratories through their high school where they could make just about any readily synthesized chemical, including highly poisonous and/or explosive compounds. More than a few made homemade explosives. Some distilled their own high-test "moonshine". The mechanically oriented made their own "go-carts" and raced them on the back streets of the suburbs. Others built and launched homemade rockets (not the super-safe kind you can buy at hobby stores, but large ones using exotic propellants). Some just played with commercial explosives out in the woods or hills. This was an era when farmers could still buy dynamite (for clearing stumps and rocks from fields) by the box at the local hardware store without a federal permit. Today "educational" activities such as those described would land the students in juvenile detention centers.

The "Rocket Boys" in the true-life movie <u>October Sky</u>, [130] through a series of experiments that often destroyed property and endangered the lives of innocent passersby, yet continually encouraged by their high school science teacher, developed the technology to launch man-sized rockets more than two miles straight up. Their description of these experiments took first prize at the National Science Fair. They would almost certainly have been jailed as terrorists (or at least dangerous youthful offenders) if they had conducted the same experiments today. Furthermore, their teacher would have been dismissed if not arrested for contributing to the delinquency of minors. Nevertheless, those experiments got all of the Rocket Boys out of mining town poverty (by guaranteeing them college scholarships) and led two of them into engineer careers. As a high school student in the sixties, the author could legally buy any chemical (including poisons, oxidizers, fuels, corrosives, and/or biological growth media) in any laboratory-scale quantity (typically decaliters of liquids and kilograms of solids) except for controlled substances (narcotics). Today, with a Ph.D. in applied science (but essentially chemical physics), few of the major chemical supply houses will sell him any quantity of even relatively benign chemicals, unless he purchases them through his institution, for fear of the supply houses being prosecuted as abetting potential terrorists or designer drug makers. A high school kid pointing a pocket laser pointer at a police officer can be (and has been) charged with assault. Pointing it at a police helicopter at night can lead to charges of assault with intent to kill. America's quest for "safety at any price" has closed many of the avenues that created and nurtured interest in science and technology in past generations.

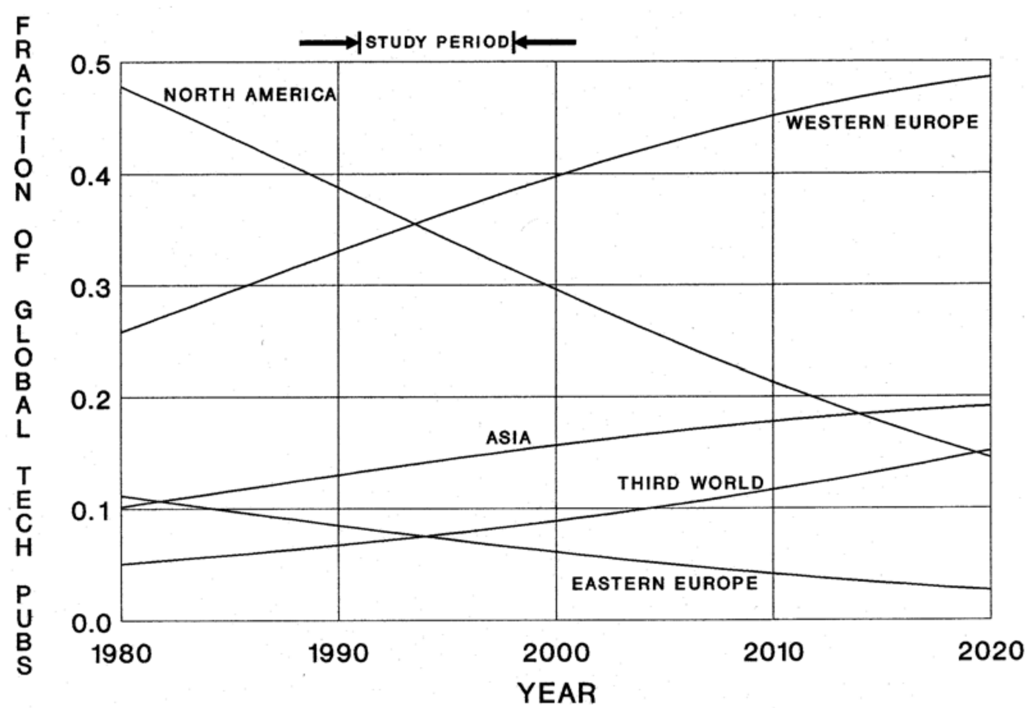
Science and technology have also lost much of the respect they once held. Progress, facilitated by scientific discoveries, has often led to large-scale problems that the scientists had not foreseen. The widespread use of DDT to control insects led to the near extinction of many species of birds. The overuse of antibiotics has led to resistant strains of disease. Nuclear power is a dying industry because poor safety practices in the past have produced a few disasters. The use of chlorofluorocarbons is now destroying the ozone layer. The burning of fossil fuels is threatening the planet with global warming. Science and technology are convenient scapegoats on which to blame the continually emerging problems. The tendency of science and technology to be associated with such problems is condemned much more than their ability to solve those same problems and to increase the standard of living of mankind is praised.

The United State Government is spending a smaller fraction of its budget on research today than it has during the last 5 decades. It is expecting industry to pick up and fund what it does not. However, industry spends very little money on basic research. Companies need to

make a profit and make that profit quickly or they go out of business. As a result, industry funds only those research areas that are almost certain to generate new products within a few years. Basic research is left to the government to fund and government funding is decreasing, even though the number of fields in which basic research should be performed is increasing.

The degree statistics cited earlier indicate that many nations already have a larger percentage of their adult populations educated in technical specialties than does the United States. This in and of itself should hint that U. S. technological superiority may be slipping. However, the results of a recent study of scientific output (as measured by numbers of technical publications) are even more shocking. A comprehensive study of technical publications for the years 1991 to 1998 indicates that the United States is no longer the dominant source of scientific discovery and technological innovation.[247] Based on the data in Reference 247, Figure 10-1 shows the fractional contribution to the total annual output of technical publications of North America (essentially the U. S.), Western Europe, Eastern Europe, Asia, and the Third World over the period from 1980 to 2020. Data for 1991 to 1998 are study data. Results prior to 1991 and after 1999 are extrapolations from the study data. Based on this analysis, in 1980, almost half of all technical publications originated in North America. By 2000, this fraction has fallen below 30% and by 2020 (barring no changes in the trends) will have fallen below 15%. The behavior of scientific output in Western Europe is almost the mirror image of the United States. By 2020 more than half of all technological innovation will be coming from Europe. This prediction is almost certainly an underestimate. The output of Eastern Europe

Figure 10-1. Percentage of global annual technical papers published by region.



fell during the 1990's because of the collapse of the Soviet Union and the Warsaw Pact. Resources previously spent on technical research were transitioned to subsistence of the population. As the economies of Eastern Europe recover, which they almost certainly will by 2020, technical publications will rebound as well. The total output of a united European Economic Community will likely exceed the extrapolations shown here. Even more shocking is the prediction that Asian contributions will be one-third larger than American contributions by 2020 that even the Third World (Latin America, Africa, Mideast, and Oceania) will have surpassed the United States in technical output. Unless drastic steps are taken to invalidate these extrapolations, America may find that it has become a technological second class citizen.

As we have shown, the technological superiority that kept the U. S. a superpower during much of the 20th Century is disappearing. Complacency, poor policy decisions, deteriorating educational systems, and the lack of a national vision of the future, to name a few of the factors, have combined to produce conditions where our national technological might has begun to atrophy. The United States will be responsible for a continually decreasing percentage of technological innovations. Since our economy is strongly dependent on developing new technologies, a relative decrease in percentage of new innovations will result in declining economic strength. Furthermore, potential adversaries will be making an increasing percentage of those innovations. The majority of innovations will be made by countries over whose exports the United States has no control and little influence. It is also possible, if not likely, that many of the decreasing U. S. innovations will be made by citizens of adversary countries, who will return home to those adversaries after a few years, taking complete knowledge of those developments with them. They might also subtly sabotage their U. S. host organizations before they depart. With proportionately fewer scientists and engineers available, the United States will be less able to respond to technological developments made and/or exploited by an adversary. Our status as technological leader of the world could decline until we were no longer even in the top ten. It is likely that our recognition as a world power will decline proportional to our atrophy in technological innovation. If things decay to a state where other countries are developing the cutting edge weapons, then our military will no longer possess the technological force multipliers on which we have grown to rely. Loss of these multipliers coupled with our diminished manpower means we will be unable to fight and win those battles deemed critical to our national security. We may become the weak sister in the North Atlantic alliance, just as we were the weak sister to Great Britain and France in World War I.

NPC should attempt to capitalize on U. S. technological atrophy as well as exacerbate that atrophy. It must build its own technological infrastructure by building world-class universities and national laboratories. Despite this, it should send as many students as practical to U. S. universities. If U. S. schools can fill their enrollments with foreign students, there will be less need to offer incentives to U. S. students. As NPC universities become better and more numerous, the better students might be kept home and poorer-performing students could be sent. If earlier NPC students were able to set the standard for learning and through their requests and comments were able to affect the curriculum, then a gradual reduction in student quality might produce a gradual reduction in overall quality at the U. S. schools. Thus, the few U. S. students who do attend the U. S. universities would receive a proportionately poorer education.

Through its substantial population of NPC citizens resident in the U. S., NPC should strive to keep the elementary and high school educational systems of the U. S. weak. For instance, they might demand that money be spent on bilingual education. Money spent in this area enriches the children of the NPC community while doing nothing for the rest of the school population. It clearly will not be available to improve the technological education of U. S. students. They might also demand more focus on the NPC cultural heritage. Again money spent on teaching NPC culture and the history of the NPC emigrants in the U. S. is money that cannot be spent on science and technology. The NPC families would not be permitted to stay in the U. S. more than five or six years, so that their children would not be too adversely affected by the poor caliber of education they received here. NPC students might be encouraged to form racial-oriented cliques and gangs. The exacerbated racial tension would detract from the general educational environment. Vandalism from these gangs aimed at the schools and the increased security to control it could further deplete school budgets.

NPC activism should target science and technology as modern bug-a-boos. The NPC community should emphasize environmental activism of the radical kind (vice the scientific kind). Even if they cannot vote, they should demonstrate for candidates whose agendas favor socialist projects (welfare, social security, Medicare, civil rights, and other big government activities) over those who favor increased support of science and technology.

The United States should reform both its educational system and its research and development infrastructure. Schools need to dramatically increase both the quantity of science and mathematics being taught at all levels, but also the "quality" or depth of what is being taught. Teachers trained in science and math should be the only ones permitted to teach those subjects. In order to guarantee an adequate supply of trained teachers, school districts need to double or triple salaries of teachers in those fields and increase the salaries of all teachers. However, there is no justification for a high school football coach to be paid more than a science teacher, a math teacher, or even an English teacher. School laboratories need to be recapitalized with up-to-date experiments and demonstrations. We probably cannot reverse our societal preoccupation with safety, despite the net benefits this might bring, so these modern labs must emphasize exciting results while maintaining an adequate degree of safety. Elementary schools must not be allowed to graduate or pass on students that cannot read, write, and do arithmetic. High schools should not graduate students that cannot critically read a novel or nonfiction book, write an intelligent discussion of that critical reading, perform all kinds of arithmetic and solve algebraic problems, and understand and adapt the fundamental concepts in the fields of physics, chemistry, and biology.

Incentives are needed to encourage the nation's youth to study science, mathematics, and engineering at the university level. These might include more merit-based scholarships usable only for science or engineering educations, increased job opportunities for U. S. students (perhaps by reducing the number of foreign visas granted to scientists and engineers), and increased graduate-level education opportunities.

The reputation of science and engineering as desirable fields needs to be rebuilt. This might be achieved in several ways. The government might fund talented writers and historians to popularize science and engineering accomplishments and the individuals who accomplished them. These works should be made available via multimedia such as the Internet and commercial television (the Government should buy the time to air them or make the stations air them as part of their public service commitment). National prizes with substantial monetary awards should be established in all fields not just the few that currently exist. Meritorious service awards should be given to all individuals who make major contributions to science and technology (not just to civil servants who are about to retire).

The government should get back into the basic research business. Basic research budgets at the NSF, DoD, DoE, NIH, etc. should be increased back to fractional levels comparable with their heydays of the 1960's or 1970's (whichever is larger). The government should practice what it preaches. Technological degrees should be required for those with oversight of technological enterprises, all the way up to Cabinet level. Civil service employees should be encouraged to obtain advanced technical degrees. All military officers at or above the level of O-4 should be required to have advanced degrees and the majority of those should be in technologically oriented fields. The government should incentivize industry to become involved in science and technology education and training by not permitting large quantities of foreign scientists, engineers, and programmers to obtain visas to either study or work here. We should strive to attract and let in only the best of the best of the foreign candidates. This will force improvements in the internal supply of candidates and reduce the number of individuals in which we invest in training merely to later compete against us.

The United States cannot afford to let its technological superiority atrophy. If we become a second-rate producer of technology, we will become a second-rate power. If we become a second-rate power, there are too many adversaries who would be willing to and capable of attacking and defeating us militarily and altering our form of government.

DISRUPTIVE TECHNOLOGIES

In the commercial world <u>***disruptive technologies***</u> ***are typically low-end technologies that lack capabilities required by major customer segments (and provided by mainstream technologies) but nevertheless find small niche markets. [131]*** <u>See Appendix M for a more detailed examination of potential disruptive technologies</u>. ***The initial niche markets may have little or no overlap with the major customer segments and the initial capabilities of the technology may not be recognized as having any relevance to the requirements of the major customer segments. However, over time these low-end technologies develop more and more capabilities until they rival the capabilities provided by the mainstream technologies and offer significant additional benefits (usually reduced costs, but possibly new capabilities such as portability). The disruptive technologies then rapidly displace the mainstream technologies in the major consumer segments. The rapid displacement of "mainframe" computers by personal computer networks in many corporate applications is a clear example of a disruptive technology at work. Many (such as DEC) in the computer business scorned personal computers until those personal computers had eaten away most of the market for the mainframes that DEC produced.***

Disruptive technologies are technologies that completely disrupt the status quo. They may be slow to develop. They may have little impact as they become established, except in niche areas, but in a military context, they have the potential to change almost every aspect of how wars are fought. For example, the tank, once its function had been truly appreciated, transformed land warfare from "attrition warfare" (defense-oriented trench warfare) to "maneuver warfare" (offense-oriented blitzkrieg). U. S. military forces invest so much effort and capital in expensive yet evolutionary high technology equipment and extensive doctrine and training at all levels in the use of that equipment, that they often cannot respond quickly when disrupting technologies arise. Leaders proficient at the old style of warfare often find it difficult to assimilate and internalize the new style. Forces trained using the older equipment may be reluctant to accept new and "untried" equipment and tactics. It may take several years before individuals become truly proficient in the new technology. Potential adversaries that are quicker to adapt to disrupting technologies can exploit this potential vulnerability in U. S. forces.

In the military arena we can consider any technology that has the potential for providing revolutionary new capabilities or quantum leap improvements in old capabilities to be a potential disruptive technology. The disruptive technology need not be developed initially for military applications. Commercial breakthroughs will become "militarized" at an exceeding rate in the future. Witness the fact that computer technology was initially driven by military needs (the first computers were used for cryptography, generation of ballistic tables for artillery, and calculation of nuclear weapon designs) yet today it is the consumer segment that is pushing microprocessor technology to ever-increasing performance.

The United States military forces are vulnerable to disruptive technologies, as are virtually all other military forces. Vulnerability to disruptive technologies is a transient process. It begins whenever an adversary develops or deploys a new capability first and ends when we

respond by matching deployments of similar capability or deployment of an effective countermeasure capability. The duration of the "window of vulnerability" depends on our ability to respond effectively, which often depends on where we were positioned in the race to develop the disruptive technology. Our existing force structure, doctrine, and traditions may make it difficult for us to develop or exploit such technologies when given the opportunity. For example, consider an adversary's development of artificial intelligence for replacing pilots in aircraft with computers. This was discussed in an earlier section of this work. If the adversary exploits this technology, then that adversary can gain an aviation capability that is as far ahead of today's U. S. aircraft capability as the aluminum monoplanes of WWII were ahead of the wood-and-fabric biplanes of WWI. The U. S. is among the leaders in both aircraft and computer technologies. By all rights, the U. S. should be the first to develop pilotless (or at least remotely piloted) combat aircraft. However, not surprisingly, former aviators dominate the leaderships of the U. S. military aviation development communities. Few attempts to eliminate pilots (and thus both the source of their own successes and the source of future military aviators) from combat aircraft are vigorously pursued by these ex-aviators. Because we are not aggressively pursuing our own development, we are offering an opening to potential adversaries, and may also be significantly lengthening the window of vulnerability that would result if an adversary pursued that opening.

In Table 10-1 we list a number of potential disruptive technologies. The table also presents an initial risk analysis of each technology. A probability of occurrence (Low/Medium/High) is assigned to each technology. A consequence of occurrence (or impact) was similarly assigned. The author attempted to limit the scope of impact assessment to militarily-related activities (although in modern society this is difficult if not impossible to do). Both of these probabilities were estimated by the author, and are obviously highly subjective. Nevertheless, the estimates were made only after careful evaluation of the current state of the art and existing trends in scientific research. The reader should feel free to assign his own probabilities to any technology with which he is intimately familiar. A subjective risk to the U. S. military was obtained by using the standard risk categorization matrix shown in Table 10-2.

Two time frames were analyzed. The first time frame was 2015. The fundamental assumption was that the technology would have matured to such an extent by this date that, at a minimum, an initial military operational capability would exist. Note that the initial operational capability might exist in an adversary's armed forces rather than in U. S. forces. Regardless of who implements a disruptive technology, the results will still be disruptive. Nevertheless, some countries will be able to implement disruptive technologies faster than others. The long development times associated with U. S. military equipment means that for an operational capability to exist in 2015, the key technology concepts and scientific breakthroughs must occur before roughly 2005. In other cultures, these breakthroughs might occur as late as 2010 and still permit an operational capability in 2015. A second time frame around 2030 was also analyzed. This time frame is far enough in the future that key technology breakthroughs need not occur for a couple of decades.

Appendix M discusses the potential military impact of each of these potential disruptive technologies. The technologies marked with an asterisk in Table 10-1 have already been discussed in earlier sections and are not discussed in detail in Appendix M. In the remainder of

Table 10-1. Potential Disruptive Technologies

DISRUPTIVE TECHNOLOGY	2015 LIKELIHOOD	2015 IMPACT	2015 RISK	2030 LIKELIHOOD	2030 IMPACT	2030 RISK
*Artificial Intelligences	MEDIUM	HIGH	HIGH	VERY HIGH	VERY HIGH	VERY HIGH
*Trans-Atmospheric Vehicles	LOW	HIGH	MEDIUM	HIGH	HIGH	HIGH
*Directed Energy Weapons	LOW	HIGH	MEDIUM	HIGH	HIGH	HIGH
*Terminally-Guided Ballistic Missiles	HIGH	HIGH	HIGH	HIGH	VERY HIGH	VERY HIGH
*Weather Control	LOW	MEDIUM	LOW	MEDIUM	MEDIUM	MEDIUM
Advanced Algorithms	MEDIUM	MEDIUM	MEDIUM	HIGH	HIGH	HIGH
Target Recognition/ID/Discrimination	MEDIUM	MEDIUM	MEDIUM	HIGH	HIGH	VERY HIGH
Micro-Electromechanical Systems (MEMS)	HIGH	MEDIUM	HIGH	HIGH	HIGH	HIGH
Z-Plane Electronics	MEDIUM	LOW	LOW	HIGH	MEDIUM	HIGH
Scalable Neural Network Chips	LOW	MEDIUM	LOW	MEDIUM	HIGH	HIGH
Direct Mind-Computer Interfaces	LOW	MEDIUM	LOW	MEDIUM	HIGH	HIGH
Very Energetic Materials	MEDIUM	MEDIUM	MEDIUM	HIGH	MEDIUM	HIGH
Electromagnetic Launch	MEDIUM	MEDIUM	MEDIUM	HIGH	HIGH	HIGH
High Energy Density Power Supplies	LOW	MEDIUM	LOW	MEDIUM	MEDIUM	MEDIUM
Bionic Augmentation	MEDIUM	MEDIUM	MEDIUM	HIGH	MEDIUM	HIGH
Ultrastrong Fibers	MEDIUM	MEDIUM	MEDIUM	HIGH	HIGH	HIGH
High-Temperature Superconductors	MEDIUM	MEDIUM	MEDIUM	HIGH	HIGH	HIGH
Cold Fusion Power Supplies	LOW	HIGH	MEDIUM	MEDIUM	HIGH	HIGH
Deep Diving Submarines	MEDIUM	MEDIUM	MEDIUM	HIGH	MEDIUM	HIGH
Quantum Computers	MEDIUM	LOW	LOW	MEDIUM	HIGH	HIGH
Passive Coherent Location	MEDIUM	HIGH	HIGH	VERY HIGH	HIGH	VERY HIGH
Ultrasensitive Magnetic Detectors	HIGH	MEDIUM	HIGH	HIGH	HIGH	HIGH
Ultrasensitive Gravitational Detectors	MEDIUM	LOW	LOW	HIGH	MEDIUM	HIGH
Active Element Conformal Arrays	MEDIUM	HIGH	HIGH	HIGH	VERY HIGH	VERY HIGH
Nanotechnology	VERY LOW	MEDIUM	LOW	LOW	HIGH	MEDIUM
Nanites	VERY LOW	HIGH	LOW	VERY LOW	HIGH	LOW
Genetic-Engineered/Cloned Warriors	LOW	LOW	LOW	HIGH	HIGH	HIGH
Fusion Power Plants	LOW	LOW	LOW	MEDIUM	MEDIUM	MEDIUM
Nuclear Catalysts	VERY LOW	MEDIUM	LOW	MEDIUM	MEDIUM	MEDIUM
Matter-Antimatter Reactors & Weapons	LOW	HIGH	MEDIUM	HIGH	HIGH	HIGH
Tectonic Weapons	LOW	LOW	LOW	MEDIUM	LOW	LOW
Gravity Control	VERY LOW	MEDIUM	LOW	VERY LOW	MEDIUM	LOW
"Warp" Drive	VERY LOW	HIGH	LOW	VERY LOW	HIGH	LOW
Psychic Weapons	MEDIUM	MEDIUM	MEDIUM	MEDIUM	MEDIUM	MEDIUM
Space Colonies	LOW	MEDIUM	LOW	HIGH	MEDIUM	HIGH

* Discussed in detail in earlier chapters.

Table 10-2. Risk Categorization Matrix

PROBABILITY OF OCCURRENCE	IMPACT OF OCCURRENCE: LOW	IMPACT OF OCCURRENCE: MEDIUM	IMPACT OF OCCURRENCE: HIGH
LOW	LOW	LOW	MEDIUM
MEDIUM	LOW	MEDIUM	HIGH
HIGH	MEDIUM	HIGH	HIGH

this section we discuss how disruptive technologies might be exploited by a competitor and how the U. S. should respond to minimize the impacts of such exploitation.

The reader should note that many of these disruptive technologies sound like science fiction. In truth since few of them are currently practical, they are science fiction. However, the reader is reminded that atomic weapons and nuclear submarines and space flight were all science fiction for decades before they became science fact (and military reality). None of the technologies listed below unequivocally violate the basic laws of physics (although one or two might prove impossible as our understanding of physics improves. A number are likely to become practical and well established within one or two decades. Most will be realized before the 21st Century is half over.

NPC should attempt to identify those technologies that are becoming or have the potential to become disruptive technologies. This will require a strategy of investment across the entire breadth of known technologies. NPC must participate in the development of those technologies that are potentially disruptive. It cannot take advantage of a disruptive technology if it is not proficient in that technology. NPC must emphasize science and technology education at all levels if it is to have a workforce capable of pursuing new technologies and capable of industrially exploiting any resulting technological developments.

A strategy of substantial investment in science and technology is probably a wise move for NPC in any event. Almost all technological developments have positive economic benefits. An educated population is necessary in any superpower. Even if military conquest is not one of NPC's goals, it can advance towards global economic power by exploiting disruptive technologies in the commercial arena.

NPC must determine the future course of each potentially disruptive technology and the probable timing of key developments. It should establish, in advance, the infrastructure that will make adoption and insertion of the "disruptive technology" as painless as possible. These actions should be disguised and dissociated from the disruptive technology to the maximum degree practical, in order to prevent the U. S. from also recognizing and responding to the disruptive technology. It should also strive to effect the adoption of the disruptive technology as soon as possible. Those countries that are masters of the disruptive technology will assume leadership positions during the transitional period.

The United States must change its military acquisition system. The current system favors evolutionary development rather than revolutionary change. Disruptive technologies represent revolutionary changes rather than evolutionary developments. Equipment acquisition times must be reduced from decades to years. It is best to keep up with, if not lead, the revolution. Lagging behind the revolution provides the most vulnerability. This will entail the taking of significant risks by program management. The system must not punish those who fail, when they take reasoned risks, or their successors will not take those risks when required. The subject of acquisition reform has been the subject of many books, and deserves to be the subject of many more, as little positive change has been observed in the last thirty years. We will not address this problem further, other than to reiterate that acquisition must be done better in the future than it is today.

It is also essential to increase the technological sophistication of the military, especially the officer corps. If senior military leaders do not demand that new disruptive technologies be exploited, then the acquisition system guarantees that they will not be exploited. Even if the need for a disruptive technology is recognized, technological sophistication is required to be able to decide how to employ that technology effectively. It would be highly desirable if a much larger percentage (at least half) of senior military leaders had advanced technical degrees. A substantial percentage should have more than one advanced degree. At a minimum every officer (technical or otherwise) should be required to undergo periodic training on the newest technologies and how they might affect the military. It might even be more beneficial than not, if major commands had a staff position equivalent to (and not subordinate to) the J2, whose responsibility would be to keep up to date on all relevant technology developments and report them back to the entire staff. This individual should spend as much effort on identifying and evaluating potential disruptive technologies, as he spends on trying to evaluate what existing technologies might be inserted into existing materiel to alleviate known problems.

Of course, none of the improvements above will be of much use if the nation continues its trend towards technological atrophy, as discussed in the preceding section. If it does we will be unable to recognize potential disruptive technologies until they are most disruptive, <u>and</u> we will not be able to respond in any fashion to minimize that disruption and the vulnerability it produces.

CHAPTER 11. CONCLUSIONS

In the preceding sections we have identified a number of potential future vulnerabilities of United States military forces. None of these vulnerabilities taken in isolation can provide an exploitative competitor the ability to establish an access denial capability. However, any one of a few critical vulnerabilities when combined with a number of the others might provide the basis for such an access denial system. Among these critical vulnerabilities are long-range antiship ballistic missiles, massive attacks by antiship cruise missiles, unmanned air superiority aircraft, and solid defenses against precision-guided weapons (using GPS or terminal guidance). When combined with lesser vulnerabilities (such as advanced mines or torpedoes or capabilities to attack our satellites, pre-positioned equipment, or strategic sealift or airlift assets), exploitation of one or more of the critical vulnerabilities should make it difficult if not impossible for U. S. forces to force entry into a denied area. The majority of the lesser vulnerabilities taken together without a critical vulnerability might also allow a competitor to deny us access, although it would be more difficult for that competitor to implement such a system.

Note that a competitor's possession of a strategic nuclear arsenal that cannot be negated by a National Missile Defense will not in and of itself create an access denial capability. It will, however, force the United States to treat that competitor with much more respect than it might otherwise. U. S. military options will be severely limited by that eventuality. We will be continually faced with determining whether our political/military objectives are worth the possible loss of Los Angeles or Chicago or New York City.

Some of these vulnerabilities will become (or already are) reality no matter what actions the U. S. pursues. Others could be easily addressed by changes in policy or by increased willingness to spend more money for defense. A number will require extensive U. S. research and development to prevent their occurrence. To maintain a position of pre-eminence the U. S. does not have to eliminate every one of these potential vulnerabilities. However, it must address the handful of critical ones, and a majority of the less critical ones. Any vulnerability that is not adequately addressed has the potential to create unacceptable casualties when and if hostilities finally arise.

The significance of failing to adequately address these vulnerabilities and of allowing one or more competitors to develop viable access denial systems needs to be pointed out. If our primary competitors develop access denial systems then U. S. influence in the competitors' regions of the world will diminish to that of a buyer and seller of merchandise. Economic influence will be the only form of influence the U. S. can exert, and this may not be that important in the future world economy. As other nations' economies grow relative to ours, the U. S. share of the world market can only diminish. If one of the competitors possesses a nuclear arsenal and hegemonic desires, we will cease to be the sole superpower in the world. This will have serious consequences for the U. S. military. If aircraft carrier battle groups are no longer able to sail anywhere in the world and lead the power projection forces, and if amphibious ready groups are no longer able to close on enemy territory and land Marines on the beaches, then what uses does our expensive Navy have? The Air Force and the Army have been hinting at this uselessness for several years. If an enemy develops his access denial system, their hints will have serious merit.

Of course, a number of the vulnerabilities will adversely affect the other forces as well. The Army is placing a growing emphasis on pre-positioned equipment afloat. Development of highly capable air defenses, unmanned air superiority aircraft, or counter-stealth systems will deny the area to our Air Force as well. The real question is whether the existence of enemy access denial capabilities negates the need for any military force that cannot deal with those capabilities. The answer is obvious. All aspects of our military must adapt to be able to cope with access denial systems or they will no longer be useful. The people will not tolerate a useless military. Since the total absence of a military is unthinkable for a "have" country, in a world filled with armed "have not" countries, the military will either change itself, or the people will change it out from under them (and not necessarily for the better). The military cannot afford to let any of the vulnerabilities continue to develop in their current fashion. The United States cannot relinquish its current place in world affairs without relinquishing much that we hold near and dear.

It is instructive to examine what vulnerabilities the "red teams" chose to exploit. Without explicitly identifying the nations studied, the list included:

1) a large nation with a booming industrial economy that will undoubtedly become a peer competitor in the coming century (denoted "peer competitor" and not identical with the hypothetical NPC of the preceding sections),
2) a second very large nation with a healthy global economy but more concerned with fostering internal stability than becoming involved in international problems that do not involve its closest neighbors (denoted "hemispheric competitor"), and
3) a third large nation with clear designs on regional dominance but lacking a healthy economy (denoted "regional competitor").

Table 11-1 compares the major U. S. vulnerabilities that the teams chose to exploit to establish a viable access denial capability. One team (peer competitor) was originally shown a small subset (less than half of the listed vulnerabilities) of this analysis, but none were shown the entire list or the DSB analysis. In general most of the vulnerabilities exploited by the teams were of their own devising. The decision to exploit any vulnerability was entirely each team's independent choice. The fact that a specific vulnerability was not exploited could be due to a team's failure to identify the vulnerability, or it could be due to budgetary and/or political concerns.

It appears that the biggest correlation lies in the area of budget. The larger the military budget, the more of our vulnerabilities an adversary is likely to exploit. It is also interesting that some choices appear to be nearly universal. However, some responses occurred for every country studied. This indicates that a potential future threat will likely have at least these elements in its future force structure. We will describe only the maritime-relevant responses. Specifically, there was increased emphasis on having a credible diesel submarine force. The richest adversary nations (near peer competitors) developed their own submarines in substantial numbers; poorer adversary nations (regional competitors) purchased relatively modern Soviet or European submarines in modest numbers. The submarines carried extremely capable, long-range torpedoes, a substantial fraction of which had wake-homing seekers. Each country invested a sizeable (but

Table 11-1. Vulnerabilities exploited by each "Red Team" in the NPS Area Denial Study. Also shown are vulnerabilities identified by the Defense Science Board.

VULNERABILITY EXPLOITED	PC	HC	RC	DSB
Attacks Using WMD				
Attack by Nuclear Missiles (ICBMs)	YES	YES	---	YES
Attack by Other Weapons of Mass Destruction	YES	YES	---	YES
Direct Attacks Against Forces				
Attack by Cruise Missiles	YES	YES	YES	YES
Attack by Ballistic Missiles or Superguns	YES	YES	YES	YES
Attack by Transatmospheric Aircraft	---	---	---	---
Attack by Naval Mines	YES	YES	YES	YES
Attack by Advanced Torpedoes	YES	YES	YES	YES
Attack by Advanced Non-nuclear Submarines	YES	YES	YES	YES
Attack by Unmanned Air Superiority Vehicles	YES	---	---	---
Attack by Infrared Anti-Aircraft Missiles	---	---	---	---
Counters to Offensive Systems				
Reliance on Stealth	YES	---	---	---
Jamming of GPS & GPS-Dependent Systems	YES	---	YES	---
Jamming of Precision-Guided Weapons	---	---	---	---
Attacks on C^4I Assets				
Attack by Electromagnetic Weapons	YES	---	YES	YES
Attack by High-Energy Lasers	YES	---	---	---
Attack by Information Warfare	YES	YES	---	YES
Attack by Antisatellite Weapons	YES	---	---	YES
Reliance on Long-Range Airborne Surveillance	---	---	---	YES
Susceptibility to Strategic Deception	YES	---	---	YES
Excessive Intelligence-Response Latency	---	---	---	---
Unconventional Methods of Attack				
Attack by Special Operations Forces	YES	---	YES	---
Limited Adverse Weather Operation Capability	YES	---	---	---
Attack by Nonlethal Weapons	---	---	YES	---
Attacks on Logistics Resources				
Limited Strategic Sea/Air Lift Capability	---	---	---	---
Reliance on Limited Overseas Basing	YES	YES	YES	---
Reliance on Pre-Positioned Equipment	---	---	---	---
Reliance on Underway Replenishment	---	---	---	---
Attacks on Societal Vulnerabilities				
Civilian Intolerance of Casualties	YES	---	YES	---
Restrictive Rules of Engagement	YES	---	YES	---
Civilian Intolerance of Unnecessary Hardships	---	---	---	---
Need for Coalition Support	YES	---	YES	---
Unequal Societal Transparency	YES	---	---	---
Treaty Limitations	YES	---	---	---
Technological Change				
Technological Surprise	YES	YES	YES	---
Technological Atrophy	---	---	---	---
Disruptive Technologies	YES	YES	---	---

PC = Peer Competitor; HC = Hemispheric Competitor; RC = Regional Competitor balanced) share of its defense budget in antiship missiles. Even the poorest country studied bought thousands of Exocet or Silkworm missiles and reasonably mobile launching platforms without straining its defense budget to the breaking point or ignoring the formation of a well-rounded military. The near peer competitor nations purchased (or developed) many tens of thousands of more modern missiles. The antiship missiles could be launched from at least five different kinds of platforms: long-range attack aircraft, littoral patrol craft, conventional surface combatants (corvette or larger), submarines, and mobile land-based launchers. Launchers were purchased in sufficient quantity to allow multiple massive attacks (1000 missiles per attack in flight at one time) to be delivered nearly simultaneously at several different points anywhere in the adversary's region of operations. Seekers on the missiles included a mix of relatively unsophisticated radar seekers (as available today) and very sophisticated advanced radar, imaging infrared, and multimode seekers (to be developed in the next 10-15 years). Each country invested heavily in naval mines. These tended to be evenly divided between deep-water CAPTOR-like mines, moored mines, shallow-water bottom mines, and surf-zone mines. Most mines were expected to possess enough intelligence to permit targeting of specific ship classes, to make sweeping difficult, and to permit mines to be remotely activated and/or deactivated.

In conclusion we have identified and discussed 36 different areas in which current U. S. forces have serious vulnerabilities. It is expected that there are others that the author has not identified. We have also described an even larger number of responses that potential competitors might make to exploit those vulnerabilities. Much current discussion in the defense community centers on the need to develop a focus (a new threat) to guide future defense development. The author suggests that rather than focusing on specific country threats, we should focus on our general vulnerabilities and attempt to reduce them. A list such as that presented here could be used to guide future research & development and procurement strategies. The intelligence community might also use it as a checklist to determine if potential adversaries are attempting to covertly develop an access denial capability. If the author can identify the vulnerabilities, so can a potential adversary. Any vulnerability the U. S. fails to address is a vulnerability almost certain to be exploited by a competitor. Failure to address our vulnerabilities in a timely fashion will have catastrophic consequences for our military and for the country.

APPENDIX A. WEAPONS OF MASS DESTRUCTION

In strict usage, the term "weapons of mass destruction (WMD)" refers to weapons of such destructive capability that a single device can kill or injure hundreds of people. It was originally envisioned to include:

- Nuclear weapons – explosives based on releasing nuclear energy (through nuclear fission or fusion) rather than chemical energy.
- Biological weapons – devices that use dispersed biological materials (infectious microorganisms or toxins) to kill, injure, sicken, or incapacitate people, plants, or animals.
- Chemical weapons – devices that use dispersed toxic chemicals to kill, injure, sicken, or incapacitate people.
- Radiological weapons – devices that use nuclear radiation from dispersed radioactive materials to kill, sicken, incapacitate, or otherwise adversely affect people.

As their potential for mass destruction has been repeatedly demonstrated, massive explosive devices (such as truck bombs) and information weapons (such as computer viruses), have been included as categories of WMD by a number of people, including some government agencies. Although these "newer" weapons clearly have the potential to kill or injure hundreds of people, we will opt for the older and more accepted usage here. In the following pages we will discuss in detail the four main categories of WMD listed above.

NUCLEAR WEAPONS

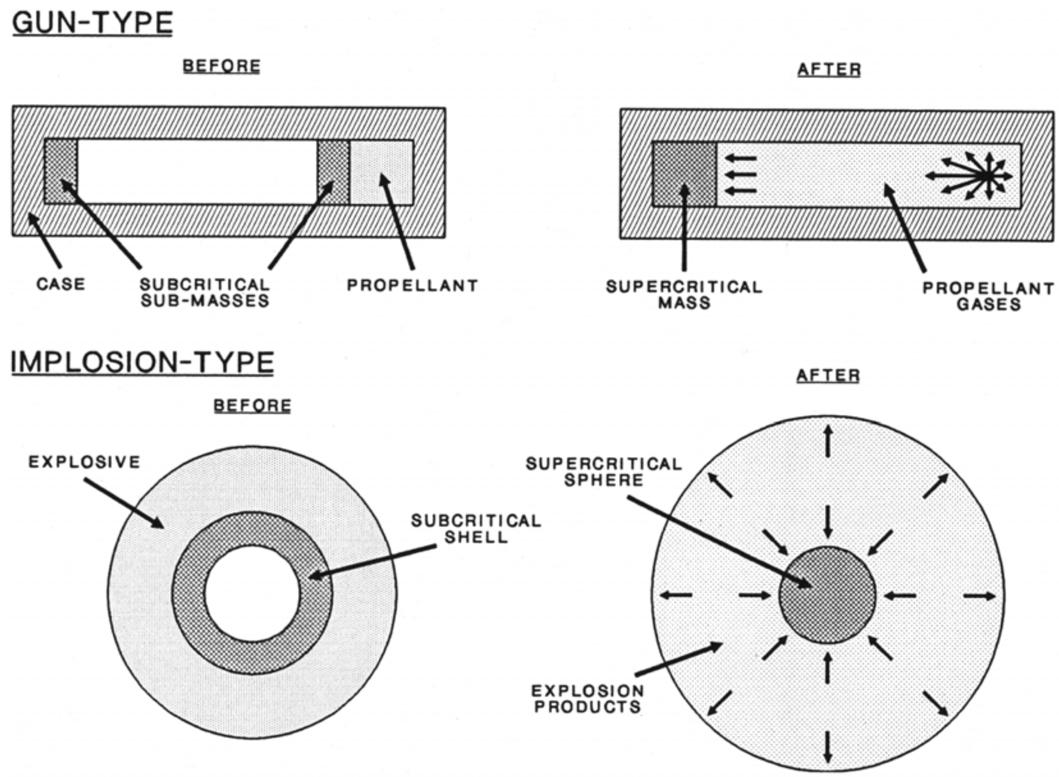
Nuclear weapons can be divided into two major categories: fission explosive devices and fusion explosive devices [132]-[137]. In fission weapons, energy is produced by nuclear fission of a fissile species such as Uranium-235, Plutonium-239, or Uranium-233. A neutron incident on a fissile nucleus causes that nucleus to split (fission) into two smaller nuclei (called fission products), releasing roughly 200 MeV of energy and 2 to 3 neutrons per fission. Complete fission of one kilogram of Uranium-235 will release roughly 20 kilotons (kT) of fission energy yield. One MeV is equal to 1.6×10^{-13} Joules and one kiloton is equivalent to 4.2×10^{12} Joules. In fusion weapons, energy is produced when two light nuclei (typically a deuterium nucleus and a tritium nucleus) combine (fuse) into a single heavier nucleus. In deuterium-tritium fusion, the reaction produces a helium nucleus, a neutron, and 17.6 MeV per fusion reaction. The neutron carries off roughly 14 MeV of the total energy released. Complete fusion of one kilogram of deuterium-tritium mix will release roughly 81 kT of fusion energy yield.

Uranium or plutonium in sufficiently large quantities will sustain a fission chain reaction. Each neutron causes fission of a uranium or plutonium nucleus with the consequent production of more than one additional neutron. The multiple neutrons from preceding fission reactions will in turn produce even more fission reactions producing a still larger number of neutrons, and so on. Some of the neutrons will escape from the mass of fissionable material without producing a fission to sustain the reaction. A fraction of the neutrons will be absorbed without producing fission. If too little fissionable material is present, neutrons are lost from the system faster than they are produced. The chain reaction will die out. However, when slightly more than a "critical mass" of material is assembled, the number of extra neutrons produced by fission will exceed the total number that escape from the mass or are absorbed without fission, and the reaction will continue to occur at ever increasing rates. Sometimes a shell of material surrounding the fissile material is used as a neutron reflector to reduce the rate at which neutrons are lost, reducing the amount of fissile material needed to create a critical mass. The bare (no reflector present) spherical critical mass for Uranium-235 is 48 kg. For Plutonium-239, the bare spherical critical mass is 10.5 kg.

The critical mass must be created from subcritical (less than critical) masses of material. Transition from extremely subcritical to supercritical (greater than critical) must occur extremely quickly (fractions of a microsecond). A supercritical mass can be assembled in two ways as illustrated in Figure A-1. In a device using Uranium-235, a solid "cylinder" of mass less than one but more than one-half critical mass can be fired from a "gun" into a hollow "cylinder" with similar mass. The aggregate "solid cylinder" of the two assembled masses will be supercritical. An alternate geometry is the use of two separated hemispheres (each containing roughly two-thirds of a critical mass). When the hemispheres are brought together, the sphere is supercritical. Gun assembly was used in the uranium atomic bomb used on Hiroshima.

For technical reasons involving excessive spontaneous fission from Plutonium-240 contaminants in the plutonium, gun assembly cannot be used with typical reactor-produced Plutonium-239. A second assembly technique involves implosion. Shaped explosive devices create an inward-directed spherical shock wave that compresses a hollow spherical shell of Uranium-235 or Plutonium-239 into a dense solid sphere. The critical mass for a spherical shell of material is considerably larger than the critical mass for a solid sphere of material. As the shell collapses it will transition from subcritical to supercritical. Implosion was used in the plutonium atomic bomb dropped on Nagasaki.

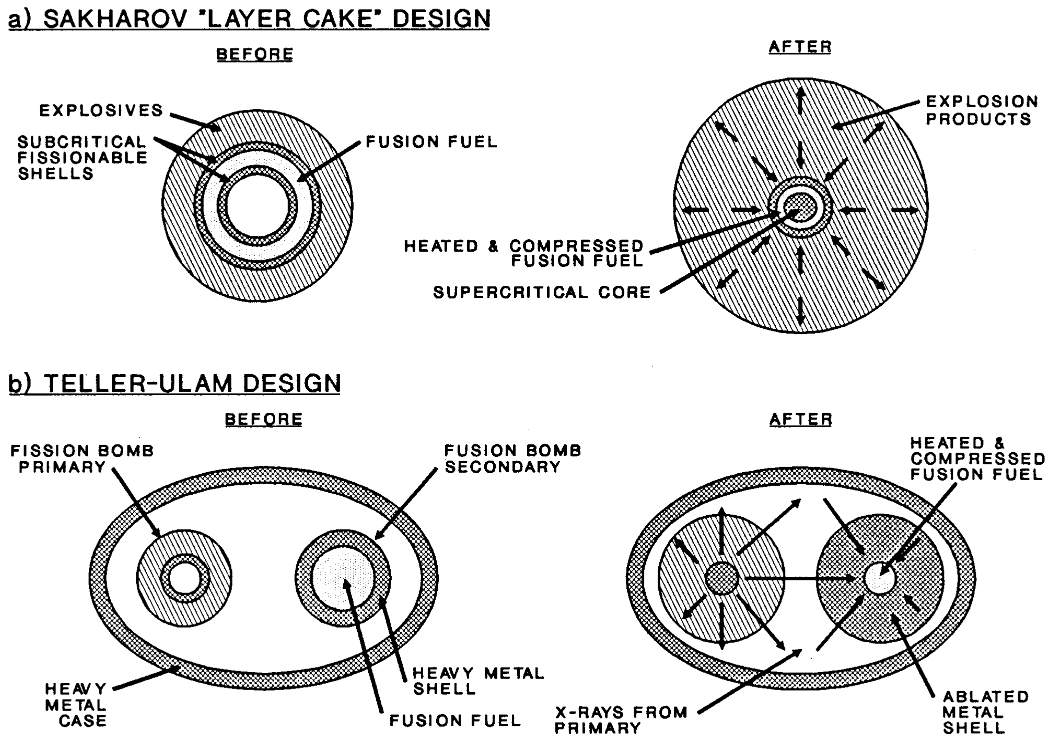
Figure A-1. Types of fission weapons: a) gun-type and b) implosion-type.



Fission weapons can range in yield from less than 1 kT to roughly 100 kT. There are few pure fission weapons. Many fission weapons have a small amount (a few grams) of deuterium-tritium gas mix at their core to enhance the fission efficiency. As the fission weapon begins to explode, the D-T mix is compressed and heated to temperatures and pressures at which fusion can occur. As the D-T mix undergoes fusion it emits an intense burst of neutrons that forces the fission chain reaction to occur at an even higher rate. The boosting produces very little fusion yield (typically less than 10% of the fission yield), but can double the efficiency at which the fission reactions occur and the ultimate yield of the weapon.

Fusion weapons come in two basic forms (Figure A-2). In the Sakharov "layer cake", several spherical shells of uranium (or other heavy metal) alternate with spherical shells of fusion fuel. The inner most shell is made from uranium-235 or plutonium. The entire spherical assembly is surrounded by explosive shaped charges to produce a spherical implosion when detonated. When the device is detonated, the shells collapse heating, compressing, and confining the fusion fuel. When the fissionable core shell collapses to a dense sphere it becomes

Figure A-2. Types of fusion weapons: a) Sakharov "layer cake" design and b) Teller-Ulam design.



supercritical. The radiation produced by this fission bomb core heats the fusion fuel to ignition. The heavy metal layers prevent the hot fuel from expanding before significant fusion occurs. The Sakharov design works and can produce weapons with yield of the order of a megaton or less. However, it has proven inferior to the Teller-Ulam design.

The Teller-Ulam design is capable of scaling to arbitrarily large yields. It places a fission explosive (the primary) and a mass of fusion fuel surrounded by a shell of heavy metal side by side inside a larger heavy metal case. When the fission device goes off, it produces x-rays which are contained by the outer shell and absorbed at the surface of the heavy metal shell surrounding the fusion fuel. As the metal surface ablates, it produces a radially outward thrust (as from a rocket) that compresses and heats the fusion fuel. When sufficient compression has been achieved the fusion fuel will ignite and produce the fusion yield.

As shown above fusion weapons require a fission device (the primary) to produce the extremely hot and dense conditions needed for fusion to occur in the fusion fuel (which is contained in a structure referred to as the secondary). X-rays from the primary heat and compress the fusion fuel to high densities and temperatures. Fusion weapons differ from "boosted" fission weapons in the quantity of fusion fuel involved. Fusion energy output from the secondary will typically exceed the fission energy yield of the primary by a factor of ten or more. The fusion fuel may be deuterium-tritium gas mix or more often it may be lithium deuteride. The advantage of lithium deuteride is that is a solid rather than a gas, so that a large mass can be stored in a small volume. Fission neutrons from the primary can interact with the lithium-6 in lithium deuteride to produce tritium that can subsequently fuse with the deuterium in lithium deuteride.

Few fusion secondaries rely entirely on fusion energy for their total yield. Many devices incorporate a blanket of depleted uranium (U-238) wrapped around the fusion core. High-energy neutrons produced in the deuterium-tritium reaction are capable of inducing fission in U-238 releasing considerable additional energy. Roughly half of the total energy released may come from U-238 fission. Large yield weapons are usually fission-fusion-fission devices. Fusion weapons can range from a few kilotons to many tens of megatons. However, typical fusion weapon yields range from 150 kT to 5 MT.

Nuclear explosive devices produce three main immediate effects: neutron and gamma radiation, thermal radiation, and blast. These three effects plus residual radiation from radioactive fallout account for almost all of the energy released. The partition of explosive yield among these effects is described in Table A-1.

Table A-1. Partition of nuclear explosive yield among the primary weapon outputs.

	Device Type		
Effect	Atmospheric Fission Weapon	Enhanced Radiation Weapon	Exoatmospheric Fusion Weapon
Blast	0.50	0.30	0.20
Thermal IR	0.35	0.20	---
Thermal X-Ray	---	---	0.70
Initial Gamma	0.03	0.10	0.20
Initial Neutrons	0.02	0.35	0.02
Residual Radiation	0.10	0.05	0.05

"Blast" in the case of the exoatmospheric weapon refers to kinetic energy carried away by fission products and gaseous remnants of the weapon structure. At short range, these particles may transfer significant momentum to any object upon which they impinge. However, there are no traditional "pressure" effects as would be associated with a blast wave in the atmosphere.

A nominal 1 kT device exploded at optimum altitude will produce 4-psi blast overpressure at 800 meters, 8-cal/cm^2 thermal radiation at 560 meters, and 300 rads, radiation dose at 950 meters. These values are nominal "threshold" values at which structural damage will be significant (from overpressure), easily combustible materials will be ignited and exposed skin will be burned severely (by thermal radiation), and unshielded individuals will get severe but frequently survivable (5-50% will die) radiation sickness (from neutron and gamma radiation). These "threshold" values are the effective radii for producing each distinct type of damage. For devices with yields (W) greater than 1 kiloton, the distances at which the "threshold" overpressure for optimum altitude bursts occurs can be shown to scale as

$$R_{blast}(W \text{ in kT}) = R(1\ kT)\ W^{1/3} = 800\ W^{1/3} \text{ in meters.}$$

The distance at which the "threshold" thermal radiation exposure occurs can be shown to scale roughly as

$$R_{thermal}(W \text{ in kT}) = R(1\ kT)\ W^{1/2} = 560\ W^{1/2} \text{ in meters.}$$

The distance at which the "threshold" radiation dose occurs does not have a simple scaling relation. However, to a very crude approximation (obtained by graphical curve fitting with no theoretical justification) we can use the expression

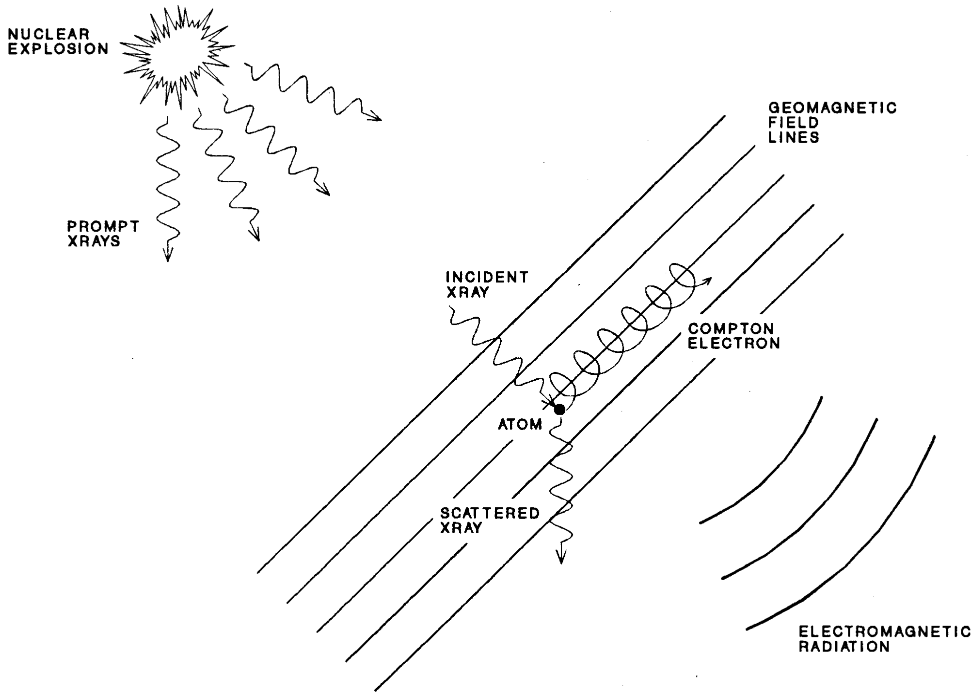
$$R_{radiation}(W \text{ in kT}) = R(1\ kT)+500\ log_{10}\ W = 950 + 500\ log_{10}\ W \text{ in meters.}$$

Thus we would expect a 1 MT bomb to have an effective blast damage radius of 8000 m, an effective thermal damage radius of 17,400 m, and a radiation injury radius of 2450 m.

The so-called neutron bomb (or enhanced radiation weapon) is a small yield fusion weapon that minimizes the amount of fission used and maximizes the amount of neutron radiation allowed to escape from the core. Less energy is contained in the nuclear fireball, resulting in less thermal radiation, less blast, and less gamma radiation output. The neutron emissions cause death or incapacitation of exposed personnel. Typically exploded at moderate altitudes, there is little thermal or blast damage. Neutron bombs must be low yield devices (of the order of 1 kT or less). Because the blast and thermal radii scale much faster with increasing yield than the radiation injury radius, at very high yields even a pure fusion weapon would produce significantly more blast and thermal damage than radiation injuries.

Nuclear weapons exploded very near the ground (<2-4 km depending on yield) or at extremely high altitudes (>30 km) can produce a phenomenon known as electromagnetic pulse (EMP) [74], [132]. Consider a nuclear explosion above the atmosphere. As there is no air to heat, the explosion produces little blast. The absence of the atmosphere means that the x-rays produced in the first few microseconds of the explosion are not absorbed in the immediate vicinity of the explosion. The lack of nearby absorption results in virtually no blast and all of the x-radiation is free to propagate to long distances. When the downward directed x-radiation hits the top of the atmosphere it is absorbed and produces energetic electrons through Compton scattering as illustrated in Figure A-3. Electrons are produced in a layer ranging from approximately 10-15 km at the lower edge to 60-90 km on the upper edge. The peak of the electron production

Figure A-3. Nuclear explosive production of the high-altitude electromagnetic pulse (HEMP).



is at about 35-40 km altitude. The high-energy Compton electrons spiral along the Earth's magnetic field lines emitting radiation electromagnetic radiation. Accelerated charges radiate electromagnetic radiation and spiral paths must have centripetal acceleration. The rapid turn-on of the radiation coupled with the moderately quick rate of energy decay of the spiraling electrons causes the emitted radiation to take the form of a short pulse of broadband electromagnetic radiation with frequencies ranging up to a few hundred MHz.

For explosions above the atmosphere, the electrons will irradiate a portion of the upper atmosphere that extends from the point directly below the explosion out to the approximate radius of the horizon (as viewed from the point of explosion – this radius is often called the tangent radius). For explosions at altitudes greater than 50 km, the radius of the electron deposition region is roughly given

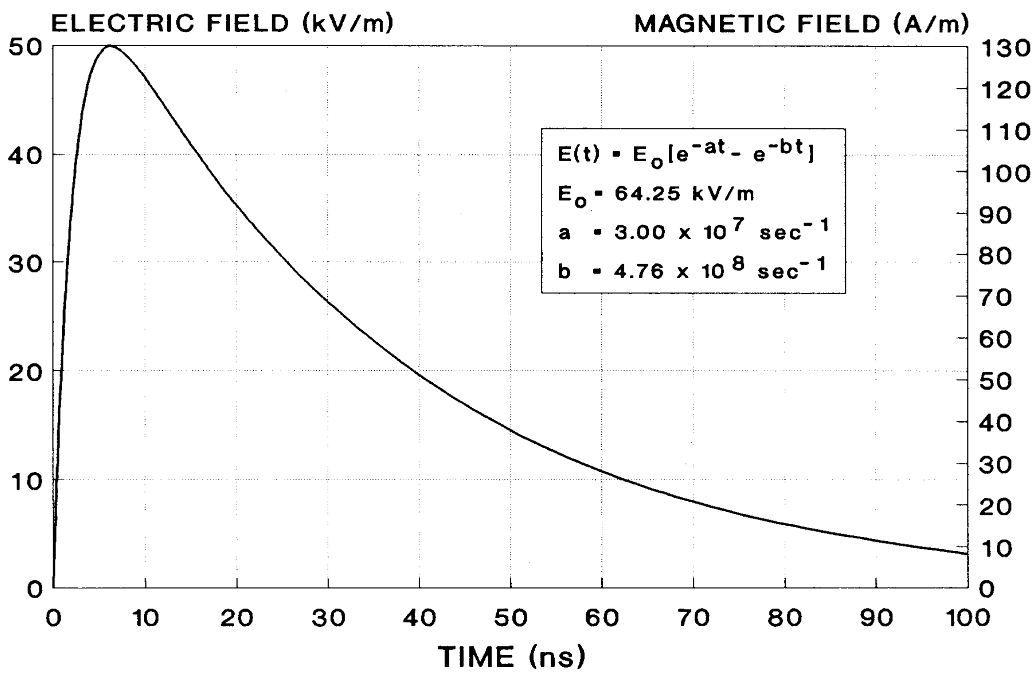
$$R \text{ (in km)} = 3.581\, H^{1/2}$$

where H is the altitude of the burst in meters. Thus, for an explosion at 300 km altitude, R = 1960 km, and the deposition area is large enough to cover almost all the continental United States. Maximum energy deposition occurs directly beneath the blast and falls off to essentially zero at the distances beyond the tangent radius R. The effective radius over which the deposition density is comparable to the peak value is roughly half the tangent radius. The geographic area under the deposition area will receive an electromagnetic pulse with an electric field that can be approximated as (times are in seconds)

$$E(t) = E_0\,[e^{-at} - e^{-bt}] = 64.25\,[e^{-30000000\,t} - e^{-476000000\,t}] \text{ (in kV/m)}$$

at its peak. This pulse shape is shown in Figure A-4. The peak field $E_{MAX} = 0.778\ E_0 = 50.0$ *kV/m* is essentially independent of the yield of the explosion. Although there is some structure including a null near but not at the point directly beneath the blast, almost all of the area within the tangent radius experiences peak field strengths that are at least 0.5 E_{MAX}.

Figure A-4. High energy electromagnetic pulse shape.

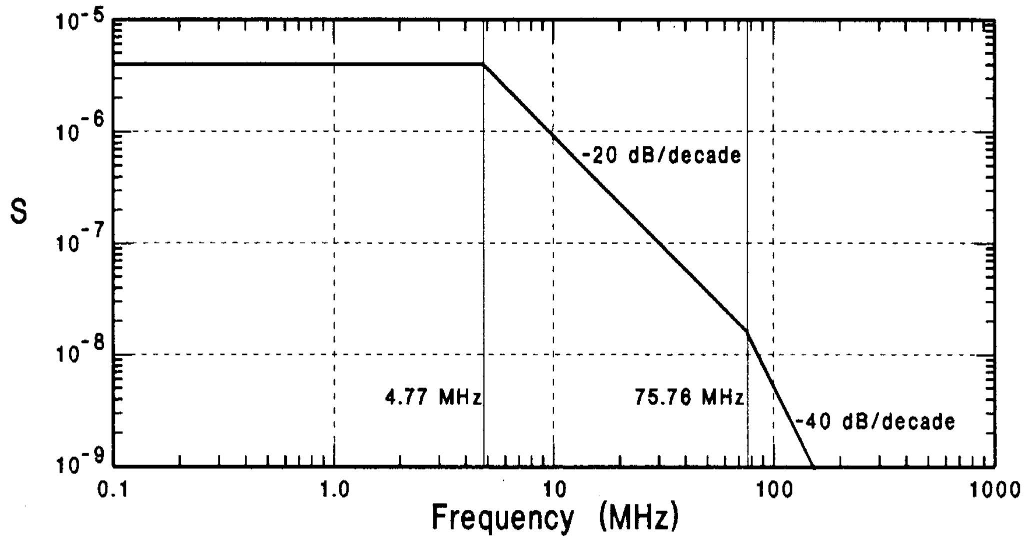


The spectrum of the radiation $S(\omega)$ (energy density vs. frequency) is given by the magnitude squared of the Fourier transform of the electric field.

$$S(\omega) = |F(\omega)|^2 = E_0^2(a-b)^2 / (a^2 + \omega^2)(b^2 + \omega^2)$$

As shown in Figure A-5 the spectrum is essentially flat until a frequency of $f = \omega/2\pi$ = 30000000/2π = 4.77 MHz is reached at which point the spectrum starts to fall off by 20 dB per decade. This fall off continues until a frequency of 476000000/2π = 75.76 MHz is reached at which point the spectrum starts to fall off by 40 dB per decade. Frequencies above 100 MHz are present but have many orders of magnitude less than those below 1 MHz.

Figure A-5. Spectrum of nuclear HEMP.



For explosions near the ground, most of the x-ray emission goes into heating the fireball and producing blast effects. It is only the initial gamma radiation that is absorbed and produces electrons within a radius R_0 that is roughly 2 times the value of $R_{radiation}$ calculated in an earlier paragraph. If the height of the explosion is considerably less than $R_{radiation}$ then more electrons are produced above the burst than are produced below the burst. The high conductivity of the earth negates the effect of any electrons produced by radiation that is absorbed by the ground. The asymmetry in the outward directed electron current allows the electron currents to radiate. Radiation outside the deposition region has a much longer pulse duration (microseconds) than high altitude EMP and has a spectrum that contains frequencies only up to about 1 MHz. The peak field strength is roughly 1 kV/m and falls off with distance as

$$E(R) = E_{MAX} R_0 / R .$$

The electromagnetic pulse will propagate out to the horizon (as viewed from the burst). Nuclear explosions at altitudes between roughly 4 km and 30 km will produce electron currents that are roughly symmetrical about the burst point. This symmetry prevents efficient radiation. The peak fields that are generated are less than 100 V/m and fall off with the same distance dependence as low-altitude EMP. The frequency spectrum is comparable to the low-altitude spectrum. Given the small initial fields and the rapid fall off with distance, the EMP from medium-altitude bursts will have few effects at any distance. Both low-altitude and medium-altitude bursts have strong radial electric fields within the electron deposition volume. However, in nuclear explosions with yields larger than a few kilotons, the effects of blast, thermal energy, and nuclear irradiation at the short distances involved (less than the deposition radius) usually overwhelm any effect of the radial electric field.

BIOLOGICAL WEAPONS

Biological warfare agents are the substances that are incorporated into biological weapons to give them a WMD function [135], [136], [138]-[142]. Biological warfare agents come in two distinct types: infectious microorganisms and toxins. Infectious microorganisms are "living" entities that can invade a host organism, grow and multiply, and produce a disease. Toxins are "dead" chemicals produced by living organisms that can enter the body of a target and disrupt basic life processes. A purist is tempted to classify toxins as chemical warfare agents (which they truly are) rather than biological warfare agents. However, both historical and common usage overwhelmingly favors calling them biological warfare agents.

The efficacy of a biological agent (or chemical or radiological agent as well) can be characterized by the effect produced, the dose required to produce that effect, the route of exposure that produces the required dose, and the persistence of the agent in the environment. A wide variety of effects can be produced. Specific effects will be described when specific agents are addressed. In general, the effects can be classified as either lethal or incapacitating. If the agent is neither lethal nor incapacitating, then it is of doubtful military utility.

The effective dose can be described in several different ways. The median lethal dose (LD_{50}) is the dose at which 50% of the exposed individuals will die. Similarly, the median incapacitating dose (ID_{50}) is the dose at which 50% of the exposed individuals will be incapacitated at a defined level. The effective dose for a microorganism is usually described by the number of microorganisms required to guarantee establishment of an infection. Effective doses for toxins and chemical agents are strongly dependent on exposure route. Exposure routes can vary from ingestion, inhalation, absorption through the skin, or "injection" into the bloodstream through injuries or small cuts in the skin. For ingested toxic chemicals, the exposure is expressed as the number of milligrams of toxic material per kilogram of body weight (i.e., mg/kg). If expressed solely as a number of milligrams, then a body weight of 70 kg is to be assumed. For an inhaled toxic chemical, the dose is usually expressed as a concentration-time product (e.g., mg-min/m^3). Higher concentrations inhaled for shorter times are assumed to yield the same effect as lower concentrations inhaled for longer times. This assumption is known as reciprocity. Persons with larger body weight tend to inhale more air per unit time, so explicit dependence on body weight is unnecessary. If the agent is in a vapor state and is absorbed through the skin, the effective dose is expressed as a concentration-time product. If the agent is in a liquid state and is applied directly to the skin, the effective dose is expressed as a number of milligrams (per kg or per 70-kg adult).

Persistence of biological agents can vary from seconds for some microorganisms to many years for bacterial spores. Most microorganisms have a short lifetime in air because they dry out and die or are killed by solar ultraviolet radiation. Many biological weapons are best employed at night. A few species form spores that can stay dormant for many years awaiting reintroduction into a suitable host. Gruinard Island was used by the United Kingdom in the 1940's as a test site for anthrax weapons. Massive quantities of spores remained in the soil until repeated decontamination efforts were finally successful in 1990. Toxins can blow away, be washed away by rain, or they can chemically degrade to "non-toxic" forms by reacting with environmental water (hydrolysis). If the intent is to quickly infect the enemy and later occupy his abandoned positions, then non-persistent agents (lifetime in air nominally less than one hour) are ideal. If the intent is to deny an area to use or occupation by the enemy for extended periods of time, then persistent agents (lifetime in air nominally greater than one day) are preferred.

Infectious microorganisms of biological warfare interest come from all the major classes of microorganism: bacteria, rickettsia, viruses, fungi, and parasites. However, to date there has been no known weaponization of parasites. In the remainder of this section we will describe the characteristics of the most prominent candidate agents for biological weapons.

Bacteria – These agents are one-celled organisms widely distributed throughout nature in the soil, air, bodies of living animals and plants, and dead and decaying organic matter. They require a suitable environment for growth that can include artificial environments (mixtures of water and nutrients called growth media). They may be spherical, rod shaped, comma-shaped, or spiral-shaped.

Anthrax is an acute bacterial infection of the skin, lungs, and the gastrointestinal tract. It is caused by the spore-forming bacterium *Bacillus anthracis*. The skin infection is caused by direct contact with contaminated animal wool, hides, or tissues and causes the skin to form dry scabs over the body. Untreated cutaneous anthrax has a fatality rate of 5-20%. Pulmonary anthrax results from the inhalation of the bacterial spores and causes fever, shock, and eventually death. There is a 90-95% fatality rate after symptoms appear in pulmonary anthrax. The gastrointestinal infection is cause by ingestion of contaminated meat that is not sufficiently cooked. This results in bloody stools, shock, and eventually death. All forms of anthrax are lethal if not treated immediately. The incubation period is usually one to seven days from contact. Single anthrax spores are 2 to 6 μm in size, making most of them respirable (particles are considered respirable – capable of being inhaled into the lower portions of the respiratory tract – if they are less than 5 μm in size). The tendency for spores to clump together or bind to dust particles making them larger than 5 μm may account for the low incidence of pulmonary anthrax in nature and the large effective infectious dose. The effective infectious dose is 8000 to 50,000 spores inhaled.

There are three types of **plague** (the Black Death of the Middle Ages) caused by the same bacterium, *Yersinia pestis*. The first is the bubonic plague, which is spread by wild or domestic rodents to humans through infected fleas. Typical symptoms include high fever, prostration, and shock. The lymph nodes swell markedly and frequently rupture from accumulated pus. This is extremely painful. The incubation period is from two to six days. Treatment with antibiotics is highly effective if used in the early states of the disease. Otherwise the disease is fatal. The second type of plague is the pneumonic plague, which is the airborne form of the Black plague. It is spread from infected individuals by airborne droplets containing plague organisms that gain entrance into the respiratory tract of uninfected humans. Military weapons (of any disease) would likely use an aerosol mode of transmission. It has the same characteristics as pneumonia except death usually occurs within hours after the symptoms first appear. It has an incubation period of three to four days. A third rare form of plague is septicemic plague, in which the bacterium attacks the circulatory system. This form is almost always fatal. The aerosol effective infectious dose for pneumonic plague is <100 organisms.

Tularemia or Rabbit fever is caused by the bacterium *Francisella tularensis*. The organism enters the body through breaks in the skin or from eating improperly cooked contaminated meat. Ticks are the main carriers of this disease and can transmit the bacteria to humans and animals by biting the victim. Military tularemia weapons would rely on inhalation of aerosols containing the microorganisms. The incubation period is one to ten days. Chills, fever, and swelling of the lymph nodes will appear with the nodes frequently breaking open from pus accumulation. If not treated in the early stages with streptomycin, tetracycline or chloramphenicol, this disease will cause death in approximately 40% of those infected. The effective infectious dose is 10 to 50 organisms.

Brucellosis is caused by one of several organisms of the *Brucella* genus: *Brucella abortus, Brucella mellitensis,* and *Brucella suis.* The organism can enter the body by eating unpasteurized foods, inhalation of aerosols, or through skin abrasions. Symptoms resemble influenza with fever, headache, myalgia, arthralgia, back pain, sweating, chills, and generalized weakness. The incubation period ranges from 5-60 days (typically 30-60 days). Fatalities are uncommon. The effective infectious dose is 10 to 100 organisms.

Glanders and **Melioidosis** are related diseases of animals that are also highly virulent in people. Glanders is caused by the organism *Burkholderia mallei*; Melioidosis is caused by the organism *Burkholderia pseudomallei.* In a biological attack, the *Burkholderia* organisms would most likely be disseminated as an aerosol. The incubation period ranges from 10-14 days. The diseases may take several forms, but for aerosol inhalation, the likely forms are septicemic and pulmonary. The septicemic form involves fever, sweating, myalgia, chest pain, photophobia, lacrimation, diarrhea, and tachycardia. The pulmonary form involves the same symptoms plus the successive development of bronchopneumonia and lobar pneumonia. If not treated with antibiotics, the diseases are invariably fatal. The effective infectious dose is assumed to be low (10 to 100 organisms).

Rickettsiae – Rickettsiae are intracellular parasitic microorganisms whose diseases are commonly transmitted by the bites of ticks, lice and fleas. They require living organisms as a suitable growth environment. Rickettsial agents may be spread as contaminated dusts or by release of large quantities of the appropriate vector (the insects that naturally spread the disease.

Q fever is an acute fever-producing disease that primarily affects the respiratory system and is caused by the rickettsia *Coxiella burnetii*. Humans are infected by inhaling dust particles contaminated with discharges from infected animals. Unpasteurized milk is another source of infection for humans. The incubation period is two to three weeks before headaches, weakness, severe sweating, coughing, and chest pains appear. It is an incapacitating disease that can be treated with a broad spectrum of antibiotics. A vaccine is available. The effective infectious dose is 1 to 10 organisms.

Typhus is caused by the rickettsia *Rickettsia prowazekii.* The disease is commonly spread by the human body louse. After an incubation period of 1-2 weeks, symptoms of headache, chills, prostration, fever, and general pains occur. After about 6 days, macular eruptions on the upper trunk and spread to the entire body. Without treatment, fatalities range from 10% to 40%. Except in cold, overcrowded areas, with reduced hygiene, typhus is not expected to produce epidemics. It is unlikely that typhus would be used as a terrorist WMD in the United States.

Viruses – Viruses are submicroscopic, unable to be seen by light microscopes. They can pass through filter systems that would collect even the smallest bacteria and rickettsiae. They require a living host to survive. They can be spread as contaminated dusts or aerosols. A few may be spread by release of vectors (typically mosquitoes or biting flies – nature's method of propagating the disease).

Smallpox is a disease caused by the Variola virus. It is transmitted primarily by inhalation and secondarily by contact with the rash and pustules which form as symptoms. Incubation periods average 12 days, but a quarantine of at least 16 days following exposure is suggested. Symptoms include general weariness, fevers, vomiting, headache, and backache, followed by a rash that develops into lesions, then pustules, and then scabs. Death occurs in about 30% of infected individuals. Technically, smallpox has been eliminated from the human population. However, samples of the virus still exist in laboratories in both the U.S. and Russia. Unaccounted for samples may exist in laboratories elsewhere. The buried remains of individuals killed in earlier epidemics may still contain viable viruses. Other poxviruses (such as monkeypox and camelpox) are very similar to smallpox. Genetic alteration of these other poxviruses may be able to recreate the virus. In the future, we may be able to fabricate the smallpox virus directly from its genetic sequence (which scientists have mapped in detail). For these reasons, as well as the fact that few people still possess any residual immunity from earlier vaccinations, we cannot eliminate smallpox from consideration as a biological weapon. Alternatively, monkeypox may be a useful biological warfare agent in its own right. The effective infectious dose in 10 to 100 viral particles.

Viral Hemorraghic Fevers or VHFs are a grouping of similar viral fevers. Some of these, the **Ebola** viruses, are familiar from books and movies. Others are old favorites, such as **Yellow fever** and **Dengue fever**. The effective infectious dose for Yellow Fever is 1 to 10 viral particles. Similar low infectious doses are assumed for other hemorrhagic fevers. Another one, **Hantavirus**, recently gained notoriety in the Southwest. VHF's are fever-producing illnesses usually accompanied by massive hemorrhaging. They are transmitted by contact or inhalation. Incubation periods are in the range of days, not hours. Symptoms include fever, muscular pain, headaches, prostration, hemorrhage, vomiting, diarrhea, hypotension, and shock. They are often fatal. Fatality rates can be as high as 90% given limited medical care; although the rates are usually lower if patients can be given intensive medical care.

Venezuelan Equine Encephalitis (VEE) is a disease caused by a complex of at least eight VEE viruses. In addition, there are several other equine encephalitis viruses that also affect humans. Any equine encephalitis virus is transmitted to humans by the bites of infected mosquitoes. The incubation period is from one to six days after which headaches, stiffness of the neck and spine, reduced sensibility, convulsions, and paralysis accompanied by a high fever appears. This disease can manifest itself as an encephalitis or as a generalized infection. The VEE virus is an incapacitating disease in humans. VEE could be a devastating fatal agent if employed against horses. The effective infectious dose is 10 to 100 viral particles.

There are dozens of other viruses that can cause fatal or debilitating diseases in humans. Many of these are transmitted by the bites of arthropods (ticks, fleas, lice, flies, mosquitoes, etc.). Any virus could conceivably be used as a biological weapon. However, the relative scarcity of many of these diseases (restricted to occasional outbreaks in remote areas of third world countries) and the requirement to use an arthropod vector for transmission (unless complex cell culture media are available), makes them unlikely candidates for biological weapons.

Fungi – The only fungus commonly considered as a candidate pathogen against humans is *Coccidioides immitis*, the cause of **Valley Fever** in the Southwest United States. Infection normally occurs by inhalation of dust contaminated with the fungus. The incubation period is 1-4 weeks. Symptoms include bronchitis, chest pains, fever, chills, and occasionally, death.

A number of fungi are potent anti-plant biological agents. From a military perspective these may be specifically employed to attack food crops (or economically critical plants) on a strategic scale. Among those that have been weaponized in the past include potato late blight, southern blight, rice blast, rice brown spot, black stem rust, and wheat covered smut. There are dozens of other candidates.

Toxins – Toxins are non-living poisons that are products of animals, plants, fungi, algae, or microbial cells. When inhaled, swallowed, or injected toxins will cause severe incapacitating illness, death, or both. Some toxins may cause symptoms almost immediately; others may not cause noticeable symptoms for hours or days.

Botulism is the acute, often-fatal intoxication caused by **Botulinum** toxin, which attacks the nervous system. It is contracted in many ways to include the ingestion of contaminated food or water, inhalation of aerosolized toxin, or through injection by contaminated projectiles or fragments. The onset of symptoms occurs at about 12-72 hours, or less if injected into the body, and is followed by vomiting, constipation, thirst, general weakness, headaches, dizziness, impaired vision and paralysis. Death can occur within 2-3 days without respiratory support. Respiratory paralysis is usually the cause of death. With endotracheal intubation and ventilation assistance, the death rate should be reducible to about 5%. The LD_{50} for botulinum toxin is 0.000001-0.00001 mg/kg.

Staphylococcal enterotoxins are produced by *Staphylococcus aureus*, and cause infection through ingestion of improperly handled foodstuffs. It can also be inhaled, but this would be a major indicator of deliberate attack. For aerosol inhalation, symptoms occur 3-12 hours after exposure. Inhalation symptoms include sudden onset of fever, chills, headache, myalgia, and non-productive cough. Ingestion symptoms also include nausea, vomiting, and diarrhea, in addition to those above. Septic shock and death can occur at high exposures. Symptoms may persist for up to 4 weeks. Ingested staphylococcal enterotoxin is considered as a serious incapacitating agent. The ID_{50} is approximately 0.00003 mg per person by inhalation.

Ricin is a water-soluble part of castor beans (*Ricinus communis)*. The wash from preparing castor oil contains up to five percent ricin. As little as a milligram can kill an individual. Symptoms occur 18-24 hours after inhalation exposure. Symptoms of topical (skin) exposure or implantation of ricin probably occur on this same timeframe. Small ricin-filled pellets injected covertly under the skin have been used as assassination weapons. Initial inhalation exposure symptoms are weakness, fever, cough and pulmonary edema. These are followed by severe respiratory distress and death from hypoxemia, or lack of blood oxygen, in 36-72 hours. The LD_{50} for ricin is 0.001 mg/kg. **Abrin** is a toxin extracted from rosary beans (also called precatory peas or jequirity beans – *Abrus precatorius*). It is very similar to ricin in physical characteristics, symptoms, timelines, and toxicity.

Saxitoxin is a toxin produced by "red tide" organisms and is responsible for paralytic shellfish poisoning. Many shellfish (such as clams and mussels) ingest the organisms and concentrate the toxin in their tissues. Individuals who eat the contaminated shellfish are sickened and often die. After ingestion exposure, onset of symptoms occurs in 10-60 minutes; after inhalation exposure, onset of symptoms may be seconds to minutes. Symptoms include progressive numbness of lips, tongue, fingertips, extremities and neck, general muscular uncoordination, light-headedness, dizziness, weakness, visual disturbances, memory loss, and headache. Respiratory distress and flaccid muscular paralysis are the terminal stages and can occur within minutes for inhalation or 2-12 hours for ingestion. The LD_{50} for ingestion of saxitoxin is 0.26 mg/kg; for inhalation it is 0.01 mg/kg.

There are many other biological toxins that have potential as biological weapons. These include toxins from cone-shell snails, tetrodotoxin from puffer fish, exotoxins from microorganisms (such as *Clostridium perfringens, Shigella dysenteriae, Staphylococcus aureus*), and mycotoxins from fungi (e.g., aflatoxins, tricothecene toxins).

CHEMICAL WEAPONS

Chemical warfare agents are toxic chemicals that are incorporated into chemical weapons to produce casualties [135]-[137], [143]-[148]. Chemical agents can be lethal or they can be merely incapacitating. Both lethal and incapacitating agents exist that act on many different aspects of human physiology. Some act on the nervous system; some act on the pulmonary system; some affect mucous membranes; others inhibit cellular metabolic functions. Persistence of chemical agents can vary from seconds (for gases that are lighter than air) to minutes (for rapidly evaporating liquids) to weeks or months (for viscous liquids or powders). Most chemical agents are ultimately degraded to nontoxic species by hydrolysis (interaction with environmental water), although this may take days even in liquid water for some agents. Persistence is strongly affected by temperature, humidity, and wind conditions. In the follow sections we describe the major categories of chemical agents and discuss the most significant specific agents in each category.

Nerve Agents – Nerve agents are among the most toxic man-made chemicals, hazardous in liquid and vapor states, and capable of causing death within minutes of exposure to a lethal dose. Most are odorless, colorless, and tasteless. Military nerve agents cause the inactivation of the enzyme called acetylcholinesterase that prevents muscles from contracting continuously; the muscles then receive a steady stream of "contract" signals causing them to eventually seize up and stop functioning. Death from nerve agents is caused by asphyxiation resulting from paralysis of the respiratory muscles due to muscle fatigue.

The "G" and "V" series nerve agents are second and third generation agents, respectively, having been developed in the 30's (G series) and 50's (V series). First generation agents were developed (and often used) during World War I. Both G and V agents are organophosphate compounds, similar to commercial insecticides such as parathion and malathion. Although there are 5 standardized G series agents (and there are at least a dozen non-standardized agents) and a comparable number of standardized and non-standardized V agents, detailed discussion of only 3 will suffice to cover all needed points of information.

Sarin, also known as "GB", acts within seconds of exposure, which may be through skin absorption (although this is weaker in sarin than in soman or VX), or more probably through inhalation. It is normally a liquid that is relatively nonpersistent, evaporating slightly slower than water. It is more hazardous as a vapor than as a liquid. Lethal dosages can cause death within minutes. LD_{50} is nominally 100-500 mg deposited on the skin or 50-100 mg-min/m^3 inhalation exposure.

Soman, also known as "GD", acts within seconds of exposure, which may be through skin absorption or through respiration. It is normally a liquid and is moderately persistent (days). It is hazardous as either a vapor or as a liquid. Lethal dosages can cause death within minutes. LD_{50} is nominally 50-300 mg deposited on the skin or 25-50 mg-min/m^3 inhalation exposure.

VX is much more toxic than the G series agents, acting within seconds of exposure, which may be through skin absorption or through respiration. It is normally an oily liquid and is highly persistent (up to weeks). It is equally hazardous as a vapor or a liquid. Lethal dosages can cause death within minutes. LD_{50} is nominally 5-15 mg deposited on the skin or 5-15 mg-min/m^3 inhalation exposure.

Effects of Vapor or Aerosol Inhalation

Small inhalation exposure to nerve agents will cause pinpoint pupils (known as myosis), runny nose and mild difficulty in breathing. Large exposure can cause sudden loss of consciousness, convulsions, temporary breathing stoppage, flaccid paralysis, copious secretions (sweating), and death.

Effects of Liquids on Skin

Small skin exposure to liquid nerve agents will cause localized sweating, nausea, vomiting, and a feeling of weakness. Large exposure will cause sudden loss of consciousness, seizure, breathing stoppage, copious secretions, flaccid paralysis, and death.

Binary chemical weapons are weapons in which two "harmless" chemicals are mixed in real time after weapons release (as a bomb falls or an artillery shell flies out to its target) to create a lethal chemical. All weaponized binary weapons involve nerve agents. GB and VX were the agents produced by the binary reactions in former U. S. binary weapons. Because binary weapons deliver standard agents, there is little need to discuss them further.

Blood Agents – Blood agents, often called "Cyanides", are so-called first generation agents. They are absorbed into the body primarily by breathing, although liquid contact exposure can occur. Blood agents prevent the normal utilization of oxygen by the cells and cause rapid damage to body tissues through lack of oxygen. Death is similar to asphyxiation, but more sudden. Specifically, cyanide ions block the *cytochrome a* step in the respiratory process. These agents are highly volatile and dissipate rapidly in the gaseous state (i.e., they are non-persistent). All soluble cyanide salts (such as **sodium cyanide** or **potassium cyanide**) are toxic by both ingestion and inhalation. The lethal dose for sodium cyanide is 100 mg/kg; for potassium cyanide it is 200 mg/kg.

Hydrogen Cyanide, also known as "AC", is considered one of the deadliest chemical agents. It acts immediately upon inhalation and manifests itself first in the central nervous system. Normally a vapor, it is nonpersistent, and rapidly disperses because it is lighter than air. Lethal dosages cause death in minutes, but less than lethal amounts produce few serious effects. Cyanide may possibly have an odor of burnt or bitter almonds. Unfortunately, about half of the population is genetically unable to detect the odor of cyanide. The LD_{50} of hydrogen cyanide is approximately 1.0 mg/kg. The LCt_{50} is 2500-5000 mg-min-m^3.

Cyanogen Chloride, also known as "CK", is a close relative of Hydrogen Cyanide. It causes intense irritation of eyes, nose and airways and there may be an odor of burnt or bitter almonds. The LCt_{50} of CK is 11,000 mg-min/m^3.

Small exposures are not fatal because cyanides are the least toxic of the "lethal" chemical agents and cyanides are rapidly detoxified by the body. A less than lethal dosage will produce few serious effects. Doses that would be fatal if given in a single amount will not be fatal if divided and spread out over days. Effects for these smaller dosages include difficulty breathing, feelings of anxiety, agitation, vertigo, weakness, nausea, possibly vomiting, and muscular trembling. Large exposures will manifest themselves within seconds of inhalation of a high concentration of cyanide agent. There is difficulty in breathing, followed within seconds the onset of convulsions. Respiratory activity ceases within two-three minutes later and cardiac arrest follows within several minutes, and then death. Total time is about 6-8 minutes after exposure.

Choking Agents – Choking or Pulmonary agents are also first generation agents, hazardous in the vapor state, and are only effective when inhaled. Even in lethal dosages they take hours to produce symptoms and death. Choking agents cause pulmonary edema, wherein the damaged tissues produce fluids that flood the lungs and in extreme cases will essentially drown the victim.

Chlorine was the first lethal military gas. Chlorine exposure causes eye and airway irritation, difficulty in breathing, chest tightness, productive cough, and pulmonary edema. It has the characteristic odor of chlorine (like hypochlorite bleach or a freshly treated swimming pool). The median lethal dosage LD_{50} is 19,000 mg-min/m^3 by inhalation exposure.

Phosgene, also known as "CG", has essentially the same symptoms as chlorine. However, contrary to chlorine, upon cessation of exposure, all symptoms may disappear for a period up to 24 hours in length, at the end of which pulmonary edema progresses rapidly often resulting in death. The vapor is four times heavier than air, is initially white in color, but soon turns colorless, and has the characteristic odor of newly mown hay. The median lethal dosage LD_{50} is 3200 mg-min/m^3 by inhalation exposure.

Small exposures to chlorine will produce immediate eye and airway irritation. Small exposures to phosgene will show little or no immediate symptoms. Again the breakdown of the alveoli and capillaries in the lungs caused by choking agents usually takes several hours to begin to manifest itself. Damage from phosgene will take much longer to show itself than damage from chlorine. A productive cough and apparent edema of the lungs will result from sublethal exposures. Large exposures to either chlorine or phosgene shows immediate eye and airway irritation. The breakdown of the alveoli and capillaries in the lungs begins to occur as quickly as 1 hour with high concentrations, but usually takes three to four hours to begin to manifest itself. During this buildup period, other symptoms from phosgene exposure may disappear; the irritant properties of chlorine are so strong that symptoms will not completely disappear. In either case, the fluid buildup is more than the normal drainage capability of the lungs, and they fill up, as in pneumonia, and drown the victim. Death usually occurs within 24 hours.

Vesicants – Vesicants or Blister agents were not meant to be fatal; rather they were meant to be debilitating and to require extensive supportive care. Nonetheless, the blister agents proved to be twice as toxic as phosgene, and are lethal in liquid and vapor states. Symptoms may not manifest themselves for many hours, but invisible damage to tissues begins immediately upon contact and continues to get worse, the longer contact is maintained. Once symptoms have begun to show, these agents cause redness and large water blisters on exposed skin and irritate the throat and lungs, eyes and other mucus membranes. Their effect on exposed tissues is somewhat similar to a corrosive chemical such as lye or a strong acid. Vesicant agents will have either a highly irritating geranium odor or smell like onions or garlic, depending on the agent.

Mustard, also known as "HD", is considered by many to be the ideal chemical agent. It attacks through inhalation and on skin contact, either as a vapor or a liquid. An oily liquid, it is highly persistent. The agent acts quickly upon contact, although its symptoms do not begin to appear for several minutes to hours, depending on the concentration and the effected tissue. It is seldom fatal, although pulmonary complications can cause death, if the mustard is inhaled. The median lethal dosage LD_{50} is nominally 7000 mg deposited on the skin or 1500 mg-min/m^3 by inhalation exposure. An eye exposure of only 200 mg-min/m^3 will cause long-term incapacitation in 50% of exposed individuals.

Lewisite, also known as "L", is quite similar to mustard. It is an oily liquid and is more volatile than mustard. It causes immediate pain and/or irritation, to the point that the victim will seek to remove it. Lewisite vapors are so irritating that victims will immediately try to leave the area. The median lethal dosage LD_{50} is nominally 1400 mg deposited on the skin or 1200-1500 mg-min/m^3 by inhalation exposure. Incapacitation through eye exposure occurs at a median dose of 300 mg-min-m^3.

Effects of Vapor or Aerosol Inhalation

Small inhalation exposures to vesicants will produce irritation, burning, and necrosis of mucus membranes in the nose, mouth, throat, and airway. The extent of damage is dependent on dosage. There may be an unproductive cough. Large exposures will produce irritation, burning, and necrosis of mucus membranes in nose, mouth, throat, and airway to include the lungs and lower bronchi if the dosage is fatal. Pulmonary edema is not usually present unless the damage is very severe. The pulmonary edema is usually hemorrhagic in character (rupturing of capillaries rather than simple seepage of blood plasma). A productive cough may be present. The cause of death is respiratory failure, most commonly resulting from secondary bacterial pneumonia.

Effects of Liquid or Vapor on Skin

Small skin exposures to vesicants will produce reddening of the skin (erythema), like sunburn, to include stinging pain 2-24 hours after exposure, dependent on state of the agent, humidity, temperature, and skin site exposed. Thinner, warmer, moister skin sites are more sensitive. Some blistering, with initially clear fluid may occur, depending on exposure. Large exposures will produce the same initial effects as small exposures, with larger, more aggressive blisters. These may also take the form of an area of dead tissue with blisters at the perimeter. These will take longer to heal and are more prone to infection.

Effects of Liquid or Vapor In/Around Eyes

The eyes are the organs most sensitive to blister agents and the onset period for effects is shorter. Small eye exposures will produce reddening and irritation of the eye escalating to conjunctivitis (pink eye), light sensitivity, and pain. Large exposures will include those symptoms mentioned at the small exposure level, with increasing pain and other effects within the eyeball itself, leading to serious corneal damage. The most serious damage results from liquid contamination or from self-contamination (rubbing the eyes). Additionally, there are systemic effects from large exposures to vesicants that can effect the gastrointestinal tract, the skeletal system and the central nervous system. Systemic effects include nausea, vomiting, sluggishness, apathy and lethargy.

Incapacitating Agents – Incapacitating agents are intended to be non-lethal and to produce no long-term casualties. They are intended to disorient individuals to the point that they cannot perform any function requiring intense concentration, rational analysis, or excellent hand-eye coordination. Incapacitation will last for hours to several days. Most incapacitating agents investigated to date are psychoactive drugs that induce severe hallucinations. The most likely agents are LSD and the military chemical known as BZ. These chemicals are typically colorless, odorless solids. They are effective by either ingestion or inhalation. Absorption through the skin would not be highly effective unless the agents were dissolved in DMSO (dimethyl sulfoxide). They could either be introduced into food or drink supplies, or they could be dispensed as extremely fine microcrystalline "smokes", such as from a burning munition (smoke grenade).

The symptoms of **BZ** intoxication (times are time after exposure) include:

1-4 hours:	tachycardia, dizziness, vomiting, blurred vision, confusion, and sedation progressing to stupor;
4-12 hours:	inability to respond to the environment effectively or to move about;
12-96 hours:	increasing activity, random unpredictable behavior with delusions and hallucination, gradual return to normal 48 to 96 hours after exposure.

The incapacitating dose of BZ is less than 1 mg per person. The median lethal dose of BZ is approximately 200,000 mg-min/m^3.

The symptoms of **LSD** intoxication include: early nausea, tachycardia, sweating palms, pupillary enlargement, cold extremities, nervousness, trembling or spasms, anxiety, euphoria, inability to relax or sleep, heightened awareness, exhilaration, kaleidoscopic imagery, rampant emotions, hilarity, and exultation. Profound terror or ecstasy may occur in some individuals. True hallucinations are rare. The incapacitating dose of LSD is less than 0.05 mg per person. The median lethal dose is considerably higher than 5 mg, although some individuals may experience life-threatening convulsions at doses as low as 2 mg.

Riot Control Agents – Riot control agents, also "Irritants" will only be mentioned briefly, because for the most part the use of these chemical agents will not be debilitating or cause serious harm to individuals. Their potential value is harassment, intimidation, or as a dispersal device or cover for other more deadly chemical agents. These agents are often readily available either through commercial or black-market sources. Typically "tear gas", either **CN** or **CS**, is dispersed through some type of burning munition, which presents an incendiary threat as well. They produce a temporary discomfort and eye closure through inhalation or absorption of small, micropulverized solids. They are not vapors, nor are they gases. Oleoresin capsicum, or **OC**, or pepper spray, is the hot pepper irritant, capsaicin, dissolved in a vegetable oil carrier. It is dispersed as a mist or spray.

Riot control agents cause pain, burning, or discomfort on exposed mucous membranes and skin, producing tears and irritation of the upper respiratory tract. The effects occur within seconds of exposure and last only minutes once exposure has ceased. High concentrations can cause nausea and vomiting. Any riot control agent might cause death in very young children, individuals with severe pulmonary problems, or in a closed room, as they displace the oxygen while being dispersed. The median incapacitating dosage ID_{50} is 10-20 mg-min/m^3 by inhalation exposure for CN and 5-10 mg-min/m^3 by inhalation exposure for CS. The median lethal dosage LD_{50} is 11,000 mg-min/m^3 by inhalation exposure for CN and 61,000 mg-min/m^3 by inhalation exposure for CS.

RADIOLOGICAL WEAPONS

Radiological weapons are devices that use nuclear radiation from dispersed radioactive materials to kill, sicken, incapacitate, or otherwise adversely affect people [149]-[152]. The nuclear radiation can act in two distinctly different ways. It can irradiate and penetrate the human body from a contaminated external environment or the contamination can enter the body allowing the radiation to irradiate organs and tissues from the inside.

There are four common types of nuclear radiation that can be produced by radioactive decay. Gamma rays (γ) are energetic photons or quanta of electromagnetic radiation. Gamma rays can travel hundreds of meters in air and can penetrate significant amounts of protective shielding. Alpha particles (α) are energetic helium nuclei. Alpha radiation will not propagate more than few centimeters in air or more than a small fraction of a millimeter in most materials. It cannot penetrate a sheet of paper or the dead outer layer of the skin. Beta-minus (β^-) particles are energetic electrons. Beta-plus (β^+) particles are energetic positrons (anti-electrons). Beta radiation will not propagate more than a few meters in air and or more than a few millimeters in most materials. However, as soon as beta-plus radiation is stopped in a material, the positrons (antimatter) will annihilate with regular electrons releasing two 0.511 MeV gamma rays per positron annihilated. The annihilation radiation is highly penetrating. Gamma-emitting and positron-emitting species can be used as external contaminants or as internal contaminants. Alpha-emitting and beta-minus-emitting species can only be used as internal contaminants. Alpha emitters are the most dangerous internal contaminants because alpha particles are capable of causing atomic dislocations. Such dislocations invariably create free radicals or altered chemical species that can disable key enzymes or produce toxic products. Genetic damage or mutations may result.

Internal contamination can be achieved in three ways. The radioactive active species can be inhaled as a gas or small particle. Some of the inhaled material will be retained in the lungs, where the radiation can act on lung tissue or on the blood cells flowing through the alveoli. Radioactive material can enter the body through a wound. This is a rare form of contamination but may be significant on a battlefield. Finally, the radioactive material can be ingested (swallowed). Ingestion is not limited to eating or drinking contaminated foods. Inhaled particles that are not respirable can be trapped in the mouth or throat and subsequently be swallowed. Some of the ingested material may be "digested" in the stomach and intestines and absorbed into the blood stream. Some absorbed species are preferentially used by specific organs. For example, most iodine ingested by the body goes to the thyroid gland where it is accumulated and concentrated. These materials may remain in the body for months or years. Some of the absorbed material may be processed by the kidneys and excreted from the body in urine. Some of the material may be rejected by the gastrointestinal system and be excreted by the bowels. In either of these last two cases, the material will remain in the body for one or two days. Particulate inhalation and ingestion of "accumulated and concentrated" species are the most dangerous modes of internal contamination.

External radiation agents are the only serious military threats. Military personnel have protective clothing that, if worn, would prevent ingestion or inhalation of radioactive agents, and would block all alpha radiation and all but the most energetic beta radiation. Gamma radiation will penetrate this protective clothing with little or no attenuation. If significant gamma doses are accumulated, the exposed individuals will develop acute radiation sickness within hours and become incapacitated or die. Internal contaminants are more likely to be used as terrorist or anti-population weapons. Most terrorist targets will not have protective equipment (or will not be wearing it). The targets may only receive relatively small exposure rates, so acute radiation sickness may not occur, or if it does, it may be survivable. However, the longer-term threat of future cancers and the resulting mental distress is right in line with terrorist intentions.

Effective doses for radiological agents may be expressed in rads (or centigrays; 1 rad = 1 cGy = 10 μJ/g of absorbed energy per unit of body weight) for external irradiation. Doses for ingested or inhaled radioactive materials are often expressed in grams of material or Becquerels (or Curies) of activity (1 Bq = 1 disintegration per second = 2.7×10^{-11} Ci). Any exposure to radiation produces a small increase in cancer risk. Data from the Hiroshima and Nagasaki survivors (studied from 1950 to 1990) indicates that external doses from 0.5 to 20 rads can result in 2.1% excess cancers (cancers over and above those expected in a normal unexposed population). Doses from 20 to 50 rads produced 13.2% excess cancers and from 50 to 100 rads produced 26.3% excess cancers. The expected cancer rate for unexposed individuals was 8.85%. Thus the 50-100 rad dose increased this rate to 11.18 % (= 8.85% times 126.3%), a small but significant 2.3% additional lifetime cancer rate. That is, a normal individual has 9% chance of getting cancer; an individual exposed to 50-100 rads has an 11% chance of getting cancer. The psychological impact of knowledge of an increased cancer probability is virtually impossible to estimate. The real impact of a large number of soldiers being subjected to such increased cancer rates cannot be ignored.

External radiation doses or whole body internal doses (delivered within a few days or less) of less than 70 rads will produce few, if any, acute radiation sickness effects. Doses between 70 and 150 rads will produce transient headache and nausea; death is unlikely. Doses above 150 rads may be fatal and hospitalization will be required in every instance. The median lethal dose is 450 rads. Fifty percent of those receiving this dose will die within 30 days. Doses above 800 rads are invariably fatal. Doses between 3000 and 8000 rads will provide complete incapacitation within 5 minutes, although partial recovery may occur after 30-45 minutes. Death occurs within 5 days. Doses above 8000 rads provide complete and permanent incapacitation within 5 minutes. Death occurs within 15 to 48 hours.

The permissible occupational dose rate for gamma radiation is 5 rads/year (0.0025 rad/hr for continuous exposure during 40-hour workweeks during a 50-week workyear). 25 rads is permissible in a single exposure during an emergency. Note: we have used a relative biological effectiveness of 1 to convert permissible occupational exposures in rem/year to doses in rads/year. For gamma radiation, 1 rad/year = 1 rem/year. Any extended exposure to low-level radiation that resulted in doses in excess of 5 rads could potentially subject a commanding officer to a board of inquiry for knowingly risking the health of his/her subordinates. Accumulation of 5 rads total dose is not difficult if contamination is widespread. For example, occupying a bunker for 2 days would produce such a dose if the dose rate were only 0.1 rad/hr. 5 rads could be reasonably expected to produce an 0.5% excess cancer rate in the exposed individuals.

The activity ζ of a mass of n grams of radioactive material can be calculated from the atomic weight A of the isotope and its half-life $t_{1/2}$ using the relation

$$\zeta \text{ (in Bq)} = 4.174 \times 10^{23}\ n/A\ t_{1/2}\ .$$

When exposed to a flux ϕ (in gamma photons/cm^2/sec) of gamma rays of energy E (in eV) the dose rate $d\Phi/dt$ can be shown to be approximately

$$d\Phi/dt \text{ (in rads/sec)} = 1.602 \times 10^{-14}\ \mu\, E\, \phi$$

where μ is the mass attenuation coefficient. Over the range 0.1 MeV to 2 MeV the mass attenuation coefficient for gamma rays in water (a reasonable approximation for the soft tissues of the human body) varies up and down between 0.03 and 0.04 cm^2/g. Given the small variation it is a reasonable approximation to assume a constant value for soft tissues of μ = 0.035 cm^2/g independent of gamma energy. If a quantity of n grams of radioactive material is distributed uniformly over a surface area A_C (the subscript C stands for contaminated), then the gamma ray flux at any point within a few meters of that surface is approximately given by one-half the total activity divided by the area:

$$\phi = 0.5\ \zeta / A_C\ .$$

The total dose Φ of gamma radiation received in an exposure time T is given by

$$\Phi = 3.344 \times 10^{9}\ n\, \mu\, E\, T / A\ t_{1/2}\ A_C\ .$$

For any radioactive species we may define a specific dose rate

$$d\Phi/dt|_{SP} = 4.2 \times 10^{8}\ E / A\ t_{1/2}\ ,$$

which is the dose rate per unit contamination strength (in rads/hr per kg/m^2 of surface contamination). If gamma rays are emitted in only a fraction of the decays or if multiple gammas are emitted in each decay, then E must be replaced by the average total gamma energy per decay. The value of $d\Phi_{SP}/dt$ for Cobalt-60 is approximately 105500 rads/hr per kg/m^2. This is a surprisingly small value for a serious contaminant such as Co-60. It will be difficult to contaminate a very large area sufficiently to produce radiation sickness within only a few minutes exposure. It would take 3750 kilograms of Co-60 to contaminate 1 km^2 of surface if the goal were to achieve the LD50 of 450 rads in a one- hour exposure. This amount of material could be carried in two large aircraft bombs. On the other hand only 833 grams of Co-60 would be sufficient to contaminate 1 km^2 to a level producing 0.1 rad/hour dose rate (the dose rate that would exceed permissible doses with only a 2-day exposure).

Radiological weapons are seldom viewed as militarily practical. The widespread availability of military protective clothing prevents internal contamination. Although some agents might present an external acute radiation sickness problem if the concentrations were extremely high and the exposures persisted for hours, it is assumed that military personnel could either decontaminate areas of interest or evacuate the contaminated areas before casualty-producing exposures are received. However, it should be noted that there are ways to modify standard radiological weapons to make them more effective. By mixing a strong gamma-emitter with a moderate setting-time adhesive, decontamination could be inhibited. If such agents were used in areas that could not be evacuated or used directly against protected individuals (so that the protective clothing became irreversibly contaminated) then militarily effective casualty rates might occur, but only with the passage of time. Of perhaps more military significance is the use of radiological weapons in rear areas where protective clothing may not be carried ready at hand or may not be available at all. In this case, internal contamination is likely. Radiation sickness is not the only "militarily effective" effect of nuclear radiation. Exposures that would produce a measurable increase in cancer rates cannot be neglected. If real cancer rates increased by as little as 1% in a sizeable population of soldiers from a democratic country that were knowingly and "unnecessarily" exposed to radiation, then the government and the military would be brought severely to task. Radiation levels high enough for 20 rads (the nominal 1% cancer rate increase level) to be achieved within a few days exposure would almost certainly require either evacuation or decontamination of the site. A dose rate of less than 0.5 rad/hr would be enough.

Persistence of radiological agents is highly variable. Radioactive decay will cause all radiological agents to decrease in potency by a factor of two every "half-life" of elapsed time. Agents can be dissolved in water and migrate into the subsoil, with upper layers of soil providing significant shielding. They may be washed away as particulates or as solutes. Such physical removal and/or burying are the only viable mechanisms for decontaminating radiological agents. Adhesives can be used to increase persistence of radiological agents in the environment almost to the limit imposed by their radioactive decay rates. The most significant potential radiological agents are described below.

Strontium-90 is a serious ingestion hazard and an inhalation hazard. It poses very little external radiation threat. Strontium is chemically similar to calcium and will preferentially be concentrated in bone ends. Radiation damage to the bone ends and marrow can produce blood disorders, immune disorders, and leukemia. It is a major fission product. The U. S. studied Sr-90 as a potential radiological weapon during World War II. Strontium-90 is produced as a by-product of fission. As many as 5.9% of U-235 fissions will ultimately lead to Strontium-90 atoms. Strontium-90 undergoes β^- decay to Yttrium-90 with a half-life of 29.1 years. Yttrium-90 undergoes β^- decay to stable Zirconium-90 with a half-life of 2.67 days. The Y-90 decays occur so quickly after the Sr-90 decay that they are included in the Sr-90 activity. When any Sr-90 decays, it produces a β^- with 0.546 MeV energy and later a Y-90 β^- with 2.27 MeV energy. The production and decay data are summarized in the expressions below.

$$\text{Fission} \xrightarrow[\text{Pu-239 (2.12\%)}]{\text{U-235 (5.9\%)}} \textit{Sr-90} \xrightarrow[\beta^-]{\text{29.1 y}} \textit{Y-90} \xrightarrow[\beta^-]{\text{2.67 d}} \text{Zr-90}$$

Energies: β^- - 0.546 (100%), 2.27 (100%--Y-90)

Iodine-131 is a critical ingestion and inhalation hazard. It is also a reasonable choice as an external radiation agent. After ingestion or inhalation, iodine will be biologically concentrated in the thyroid gland, an organ that is easily damaged by radiation. Thyroid damage typically results in a serious condition known as hypothyroidism, in which insufficient thyroid hormone is produced. The thyroid damage dose may be estimated from the dose required to treat the overactive thyroid diseases, hyperthyroidism and thyrotoxicosis (Graves' disease). This therapy involves partially damaging the overactive thyroid to bring its hormone outputs back to normal levels. A therapeutic dose delivered to a normal thyroid will reduce thyroid activity to abnormally low levels. The therapeutic dose is 86 μCi/g (of thyroid mass). Assuming a 20-g thyroid mass and a 20% iodine uptake factor, the total required dose is 8600 μCi, which can be produced by 70 ng of I-131. Doses of this magnitude may possibly produce thyroid cancer. Larger doses have increased probability of causing cancers. I-131 is produced in large amounts in nuclear fission. Roughly 2.9 % of fission reactions in uranium produce I-131. It can also be produced by neutron absorption in tellurium metal (followed by beta decays to I-131). The MOE for production from metallic tellurium is 0.00239.

$$\text{Reactor n} + \text{Te-130} \rightarrow \textit{Te-131} \xrightarrow[\beta^-]{25.0\text{ m}} \textit{I-131} \xrightarrow[\beta^-]{8.040\text{ d}} \text{Xe-131}$$

Energies: β^- - 0.247 (1.6%), 0.333 (6.9%), 0.467 (0.5%), 0.606 (90.4%), 0.806 (0.6%)
γ - 0.0816 (5.1%), 0.326 (5.1%), 0.364 (85.3%), 0.637 (6.9%), 0.723 (1.6%)

Cesium-137 is a serious ingestion hazard and an inhalation hazard. It is also useful as an external radiation agent. Cesium can replace potassium in the body (potassium is commonly found in intracellular fluids). Thus, Cs-137 is concentrated inside the cells and is perfectly located to cause DNA damage and damage to other intracellular biochemicals. Cs-137 is also a major by-product of nuclear fission. Over 6% of all fission reactions will ultimately produce a Cs-137 atom.

$$\text{Fission} \xrightarrow[\text{Pu-239 (6.5\%)}]{\text{U-235 (6.23\%)}} \textit{Cs-137} \xrightarrow[\beta^-]{30.17\text{ y}} \text{Ba-137}$$

Energies: β^- - 0.514 (93.5%), 1.176 (6.5%)
γ - 0.662 (93.5%)

Hydrogen-3 or **Tritium** is a significant ingestion hazard and an inhalation hazard. It poses virtually no external radiation threat.. It is easily produced in large quantities by irradiating lithium metal in a high-flux nuclear reactor. Lithium-6 absorbs an incident neutron and fissions into a tritium nucleus and an alpha particle. This production reaction has a measure of effectiveness (MOE) of 3.27 atoms per cm^3 of target material per neutron per cm^2 of thermal neutron flux per second of irradiation time. The MOE can be determined using the relation:

$$
\begin{aligned}
MOE \;=\; & [\textit{(Fractional Natural Abundance of Target Isotope)} \times \\
& \textit{(Thermal Neutron Capture Cross Section of Target Isotope)} \times \\
& \textit{(Density of Target Material)} \times \\
& \textit{(Fractional Weight of Target Element in Target Material)} \times \\
& \textit{(Branching Ratio of Absorption Reaction to the Desired Product State)} \times \\
& \textit{(Avogadro Number)}] / \\
& [\textit{Atomic Number of Product Isotope}]
\end{aligned}
$$

The total activity (in Becquerels) that is produced when the target material is irradiated in a reactor for a period of time T is equal to

$$
\begin{aligned}
\textit{Activity} &= \textit{MOE} \times \textit{Neutron Flux} \times \textit{Target Volume} \times 0.693\, T / t_{1/2} && \text{if } T << t_{1/2} \\
&= \textit{MOE} \times \textit{Neutron Flux} \times \textit{Target Volume} && \text{if } T >> t_{1/2}
\end{aligned}
$$

For example, if 10^3 cm^3 of metallic natural lithium is irradiated in a reactor with a thermal neutron flux of 10^{13} $n/cm^2/s$ for a period of roughly 3 hours (10^4 s) then a total activity of

3.27×10^{20} Bq (= 8.84×10^9 Curies)

is produced. If incorporated into "tritiated" water (HTO and T_2O), tritium is readily absorbed, retained by the body, and distributed uniformly throughout the body. It is flushed from the body through urination and perspiration. The half-life in the body is about twelve days. If incorporated into certain chemicals, such as ethanol, tritium can be made to target certain organs with somewhat more specificity than water. Any tritium that replaces hydrogen in any of the body's biochemicals can be retained for a year or longer, before ultimate elimination.

$$
\text{Reactor n} + \text{Li-6} \rightarrow \textit{Li-7*} \xrightarrow[\alpha]{< 1\text{s}} \textit{H-3} \xrightarrow[\beta^-]{12.33\text{y}} \text{He-3}
$$

Energies: β^- - 0.0186

Cobalt-60 is an ingestion hazard and an inhalation hazard. It is an excellent choice as an external radiation agent. It is easily produced in large quantities by irradiating natural cobalt metal in a high-flux nuclear reactor. The MOE for production of Co-60 from metallic cobalt is 3.36. Cobalt's only significant physiological function is as part of vitamin B-12, which the body does not manufacture. Unless the Co-60 was incorporated into vitamin B-12 before dispersal, the internal effects of Co-60 exposure will be limited to causing lung cancer or gastrointestinal cancers.

$$
\text{Reactor n} + \text{Co-59} \rightarrow \textit{Co-60} \xrightarrow[\beta^-]{5.271\text{ y}} \text{Ni-60}
$$

Energies: β^- - 0.313 (>99%)
γ - 1.173 (>99%), 1.333 (>99%)

Zirconium-95 is an ingestion hazard and an inhalation hazard. It is a good choice as an external radiation agent. Zirconium is commonly used a cladding for nuclear reactor fuel rods. Thus, Zr-95 is available in large quantities from reprocessing of nuclear fuel rods. The MOE for production of Zr-95 from metallic zirconium is 0.000581. Iraq attempted to weaponize at least one radiological weapon (an airplane bomb) incorporating Zr-95 made from zirconium oxide. It is believed that the zirconium activity in the Iraqi material was significantly augmented by production of Hafnium-181 from an impurity in the zirconium oxide. Zirconium is not concentrated in any specific organ in the body. The effects of ingestion or inhalation will be the production of lung or gastrointestinal cancers.

$$\text{Reactor n} + \text{Zr-94} \rightarrow \textit{Zr-95} \xrightarrow[\beta^-]{64.02\text{ d}} \textit{Nb-95} \xrightarrow[\beta^-]{34.97\text{ d}} \text{Mo-95}$$

Energies: β^- - 0.160 (100%), 0.365 (49%), 0.397 (49%), 0.886 (2%)
γ - 0.235 (2%), 0.724 (49%), 0.756 (49%), 0.765 (100%)

Hafnium-181 is an ingestion hazard and an inhalation hazard. It is a good choice as an external radiation agent. Hafnium is a common impurity in zirconium oxide. The MOE for production of Hf-181 from metallic hafnium is 0.22 (much larger than that for Zr-95 so that a 0.1% Hf impurity will produce more activity than the zirconium itself). Hafnium is not concentrated in any specific organ in the body. The effects of ingestion or inhalation will be the production of lung or gastrointestinal cancers.

$$\text{Reactor n} + \text{Hf-180} \rightarrow \textit{Hf-181} \xrightarrow[\beta^-]{42.4\text{ d}} \text{Ta-181}$$

Energies: β^- - 0.408 (93%), 0.404 (7%)
γ - 0.133 (93%), 0.136 (79%), 0.346 (13%), 0.482 (79%), 0.619 (7%)

Iridium-192 is an ingestion hazard and an inhalation hazard. It is a good choice as an external radiation agent. Iridium has no physiological function in the body. Internal exposure hazards are lung cancer and gastrointestinal cancers. Ir-192 has two decay modes which must be considered. Ir-192 can be produced by neutron absorption in metallic iridium. The MOE for producing Ir-192 from metallic iridium is a sizable 20.4.

$$\text{Reactor n} + \text{Ir-191} \rightarrow \textit{Ir-192} \xrightarrow[\beta^-]{73.83\text{ d}} \text{Pt-192} \quad (95.6\%)$$

Energies: β^- - 0.253 (4.5%), 0.532 (42%), 0.668 (49%)

γ - 0.136 (0.4%), 0.296 (29.4%), 0.308 (31.0%), 0.316 (85.6%), 0.468 (47.0%), 0.589 (3.9%), 0.604 (8.8%), 0.612 (5.6%), 0.885 (0.4%)

$$\text{Ir-192} \xrightarrow[\text{EC}]{73.8\text{ d}} \text{Os-192} \quad (4.4\%)$$

Energies: γ - 0.201 (0.5%), 0.206 (4.2%), 0.283 (0.2%), 0.375 (0.5%), 0.485 (3.4%), 0.489 (0.2%)

Plutonium-238 is not the world's deadliest material as the popular press would have everyone believe. However it is a major inhalation hazard. The high alpha radiation output almost guarantees that inhalation and retention of a few thousand small particles will result in lung cancer. Extrapolating from measurements for Pu-239, it is estimated that the cancer production rate is 3600 cancer deaths per milligram inhaled (Pu-239 is 12 deaths per milligram inhaled – see below).[253] The largest particle of plutonium that can be inhaled is about 3 micrometers in diameter and has a mass of 0.14 ng. Inhalation of one such particle would result in a 0.05% chance of getting cancer. Pu-238 is only a minor ingestion hazard because plutonium is not readily absorbed by the gastrointestinal system (only 1 part per 100,000 parts of PuO_2 ingested is retained by the body). It is not a significant external radiation hazard. Pu-238 is commonly used in radioisotope thermal generators. It is produced in large quantities as a by-product of producing or using plutonium in nuclear reactors. There are several formation pathways:

$$\text{Pu-239} \xrightarrow[\text{n,2n}]{} \text{Pu-238}$$

$$\text{U-238} \xrightarrow[\text{n,2n}]{} \text{U-237} \xrightarrow[\beta^-]{6.75\text{d}} \text{Np-237} \xrightarrow[\text{n capt}]{} \text{Np-238} \xrightarrow[\beta^-]{2.12\text{d}} \text{Pu-238}$$

$$\text{U-235} \xrightarrow[\text{n capt}]{} \text{U-236} \xrightarrow[\text{n capt}]{} \text{U-237} \xrightarrow[\beta^-]{6.75\text{d}} \text{Np-237} \xrightarrow[\text{n capt}]{} \text{Np-238} \xrightarrow[\beta^-]{2.12\text{d}} \text{Pu-238}$$

$$\text{Pu-239} \xrightarrow[\text{n capt}]{} \text{Pu-240} \xrightarrow[\text{n capt}]{} \text{Pu-241} \xrightarrow[\beta^-]{15\text{y}} \text{Am-241} \xrightarrow[\text{n capt}]{} \text{Am-242} \xrightarrow[\beta^-]{16\text{h}} \text{Cm-242} \xrightarrow[\alpha]{163\text{d}} \text{Pu-238}$$

The first two modes are more probable than the third and fourth modes. Which mode is dominant depends on whether Pu-239 or U-238 is more abundant in the reactor core. In a plutonium production reactor U-238 is more abundant and the second reaction is the dominant route. In a plutonium power reactor, the first reaction will dominate. In a highly enriched uranium power reactor the third mode may dominate. Any absorbed plutonium is concentrated in the liver and bones. Liver disease, bone cancer, and leukemia are likely to result from significant ingestion.

$$\text{Enriched } Pu\text{-}238 \xrightarrow[\alpha]{87.7\ y} U\text{-}234$$

Energies: α - 5.359 (0.11%), 5.454 (28%), 5.498 (72%)
γ - 0.0435 (28.1%), 0.1433 (0.11%)

The behavior of ordinary plutonium (Pu-239) is virtually identical to that of Pu-238. However, due to its much longer half-life (24390 years vs. 88 years) and slight lower alpha particle energy (5.15 MeV vs. 5.48 MeV), Pu-239 is 300 times less effective as a radiological agent than Pu-238. The primary advantage favoring Pu-239 as a radiological agent is that it can be obtained in much larger quantities than Pu-238. On the other hand, Pu-239 can be used to make a nuclear explosive, a much more significant use than incorporation into a radiological weapon.

Uranium-238 or **Depleted Uranium** is a significant ingestion hazard and a significant inhalation hazard. It is produced in enormous quantities as a waste product during the enrichment of uranium in the isotope U-235. U-238 does not pose any serious external radiation source hazard. Uranium is readily absorbed by the gastrointestinal system. The absorbed uranium tends to concentrate in the bones & the kidneys. Bone cancer, renal cancer, leukemia, and lymphatic disorders are common long-term by-products of uranium ingestion. In pregnant women ingested uranium can cross the placental barrier and lead to birth defects. If inhaled uranium is in an insoluble form (such as the oxide), inhaled particles may be retained intact in the lung and can result in lung cancer.

$$\text{Depleted } U\text{-}238 \xrightarrow[\alpha]{4.47 \times 10^{9}\ y} Th\text{-}234$$

Energies: α - 4.036 (0.23%), 4.149 (22.4%), 4.196 (77.4%)
γ - 0.0495 (22.4%)

WMD DELIVERY MECHANISMS

Weapons of mass destruction can, in principle, be delivered by all common forms of weapons, even rifle bullets (although poison bullets are forbidden by The Hague Convention of 1899). However, some delivery mechanisms are more suited to one form of WMD than to another. Table A-2 lists all of the major delivery mechanisms for weapons of any kind (other than small arms) and comments on the applicability of each mechanism to each kind of WMD. The author has underlined those threats that he believes may make a significant contribution to a naval access denial capability.

The diversity of possible and practical WMD delivery mechanisms is much larger than simple bombs or ballistic missiles, as commonly envisioned. Any obsession on one delivery mechanism on the part of our military planners will likely open the door to a creative, asymmetric response on the part of an adversary. To demonstrate this diversity in way not readily discernible from Table A-2, we will describe a few representative delivery mechanisms in detail.

There are many forms of "artillery" delivered weapons. Figure A-6 shows a typical artillery shell capable of delivering chemical, biological, or radiological (CBR) agents. A standard metal artillery shell case is filled with the agent in liquid (or powder) form. A small burster charge of explosives is placed at the center of the shell case. Together with the fuze assembly, the shell case and the burster charge serve to hermetically seal the agent into the artillery shell. The fuze is optimally altimetric in function and serves to detonate the shell at a height above ground that will guarantee optimum dispersion of the agent. Too high and the agent will not exist in effective concentrations at the ground. Too low and the area covered with agent will be smaller than desired. The explosive atomizes the liquid (or powder) agent and creates a wide cloud that settles on the positions being attacked. Timed fuzes or impact fuzes may also be used but usually result in less than optimal dispersion. A CBR mortar shell would look and act very similarly to an artillery shell, except that tail fins would be present to stabilize the round in flight. The artillery shell shown in Figure A-6 is spin-stabilized in flight, the spin being imparted by the rifled barrel of the gun. CBR artillery shells have been manufactured for almost every size of gun from 75 mm up to 240 mm.

Figure A-6. A nominal artillery shell for CBR agent delivery.

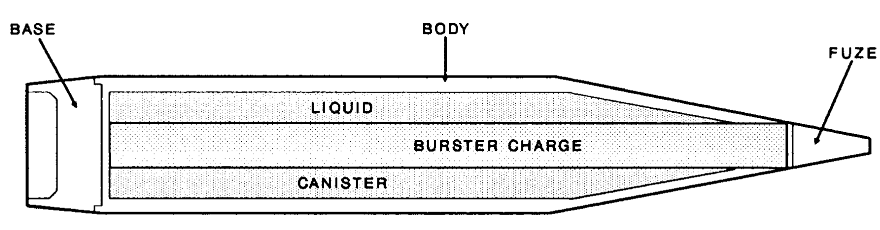


Table A-2. Delivery methods of weapons of mass destruction.

DELIVERY METHOD	TYPE OF WMD NUCLEAR	BIOLOGICAL	CHEMICAL	RADIOLOGICAL
Aerial Bomb - Unitary Warhead	*Yes	Yes	Yes	Yes
Aerial Bomb - Submunitions	No	*Yes	*Yes	Possible
Aerial Bomb - Spray-Type	No	*Yes	*Yes	Possible
Aircraft Spray Tank	No	*Yes	*Yes	Possible
Vehicle Spray Tank	No	Yes	Yes	Possible
Ballistic Missile Warhead (Non-separating Reentry Vehicle)	Yes	*Yes	*Yes	*Possible
Ballistic Missile Warhead (Separating Reentry Vehicle)	*Yes	*Yes	*Possible	Possible
Artillery Rocket or Cannon Shell	Yes	Yes	*Yes	Possible
Mortar Shell	Unlikely	Yes	*Yes	Possible
Cruise Missile - Unitary Warhead	*Yes	Possible	Possible	Possible
Cruise Missile - Submunitions	No	Yes	Possible	Possible
Anti-Personnel Land Mine	Possible	Yes	Yes	Possible
Demolition/Denial Munition	*Yes	Possible	Possible	Possible
Naval Mine	Yes	**Yes	**Possible	Possible
Torpedo	*Yes	Possible	Possible	Unlikely
Antiaircraft Missile Warhead	Yes	Possible	Unlikely	Unlikely
Transportable Bomb (Clandestine)	*Yes	**Yes	**Yes	Possible

* Major Threat

** Could be significant threat

Yes – Evidence of weaponization in this form.

No – Not possible or not practical.

Possible – No evidence of weaponization in this form but physically possible & useful.

Unlikely – Physically possible; utility seems too low to warrant weaponization efforts.

An artillery shell designed for dispensing binary chemical agents is shown in Figure A-7. It is very similar to a unitary agent artillery shell except that it has two liquid canisters, one for each of the binary chemicals. The two canisters are separated by disks that will rupture under a very high acceleration loading. When the artillery shell is fired, the launch acceleration ruptures the disks separating the two chemicals. The spin of the projectile causes the binary chemicals to mix. The ensuing chemical reaction produces the toxic agent. After formation of the agent, binary shells behave exactly like unitary agent shells.

Figure A-7. An artillery projectile for delivering binary chemical weapons.

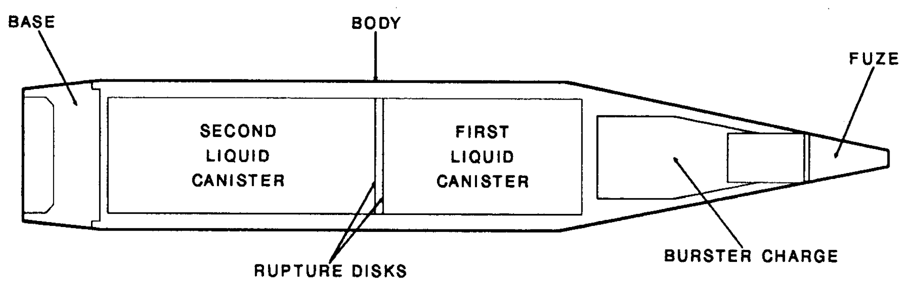


Figure A-8 illustrates a typically artillery rocket for disseminating CBR agents. These rockets are typically launched in large numbers from simple tube launchers. At launch the rocket motor ignites and propels the rocket out of the tube. Upon leaving the tube, fins unfold from the body to provide stabilization. The front half of the rocket is designed very similarly to a CBR artillery shell with agent surrounding a burster charge. After the rocket motor burns out, the projectile follows a ballistic trajectory. At the desired altitude (or time after launch or on impact – depending on the fuze), the burster charge detonates and disperses the agent. The U. S. M55 115mm rocket was a typical example of this type of weapon.

Figure A-8. An artillery rocket for disseminating CBR agents.

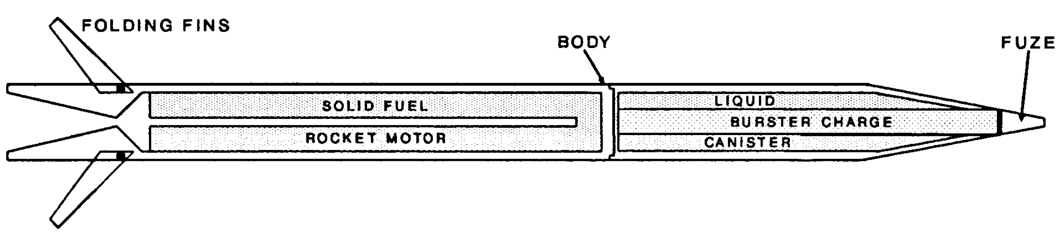
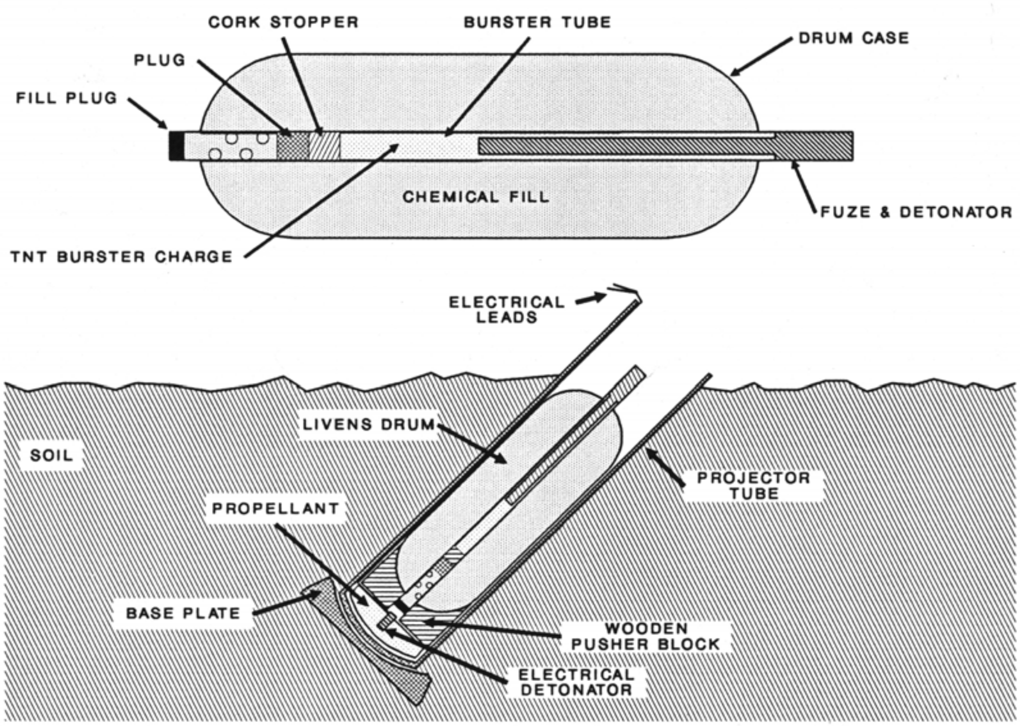


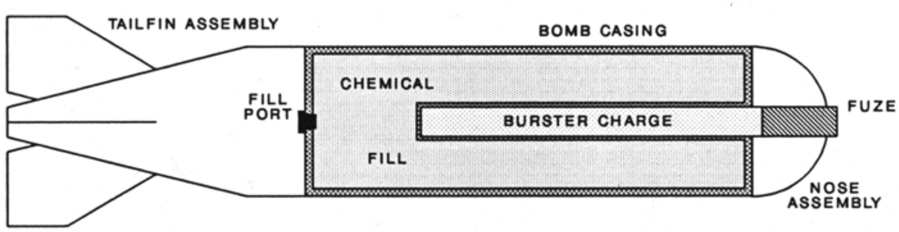
Figure A-9 shows a Livens projector and its projectile. The Livens projector is a kind of mortar. Originally designed to deliver chemical weapons, it can be used to deliver other CBR agents. A large sausage-shaped drum is filled with agent and fitted with an impact fuze and a small burster charge. A large piece of metal "sewer pipe" is fitted with a heavy baseplate and buried in the ground, angled at roughly 45 degrees and pointed at the enemy positions. An electrically-ignited powder charge (propellant) is placed at the bottom of the sewer pipe and a wooden pusher block (shaped to fit the bottom of the projectile) is placed on top of the powder charge. The Livens projectile is then lowered onto the pusher block. Typically dozens of projectors are wired in parallel. When the powder is ignited, the expanding gases accelerate the pusher block down the tube carrying the projectile with it. The barrage of projectiles can be thrown many hundreds of meters towards the enemy. When each projectile impacts the ground, the burster charge spreads the agent for tens of meters around the impact point.

Figure A-9. The Livens projector and its projectile.



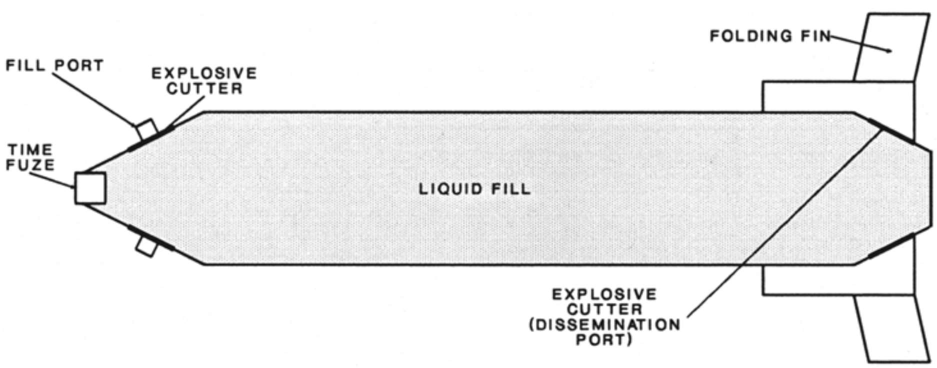
Aircraft-delivered weapons can also take a variety of forms. Figure A-10 shows an aircraft bomb capable of explosively disseminating CBR agents. A cylindrical bomb case is filled with liquid or powder agent through a fill port. A burster charge is inserted into a cavity in the bomb case and an aerodynamic nose containing the fuze is added. A tail fin assembly is added opposite the fuze to stabilize the aerodynamics of the weapon. At a pre-determined altitude (or possibly a fixed delay after release), the burster charge is detonated releasing a cloud of agent over the target being attacked. The burst altitude is selected to optimize the dispersion of the agent over the target.

Figure A-10. A nominal aircraft bomb for explosive dissemination of CBR agents.



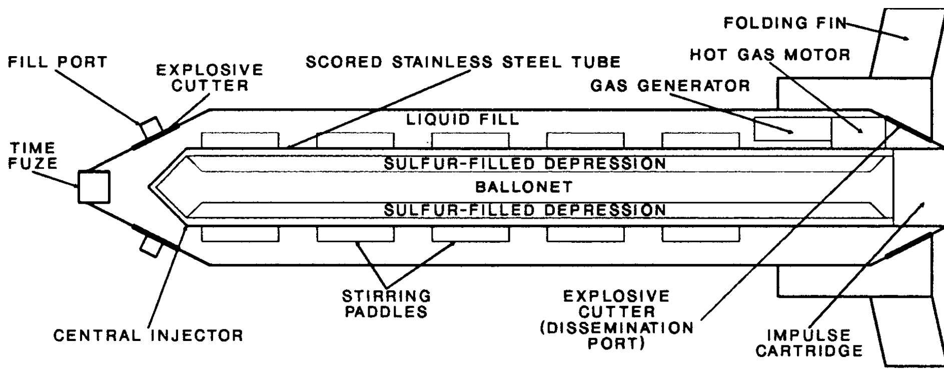
Explosive bombs produce localized roughly spherical clouds of agent. Figure A-11 shows an aircraft bomb that produces a long linear cloud of CBR agent using a spray technique. The bomb is little more than a large cylindrical tank for holding the agent, with fins for stabilization and a fuze for initiating the spray. When the fuze decides that the altitude or the time after release is correct, explosive cutters (tiny linear shaped charges of explosive) are detonated. These cut small holes in front and the back ends of the tank. Ram air pressure then forces the agent out through the holes in the rear. The agent is atomized by the aerodynamic forces. A linear cloud of agent is produced until the tank is exhausted. Typical line lengths from such a "bomb" will be several hundred meters long.

Figure A-11. A nominal aircraft bomb for spray cloud dissemination of CBR agents.



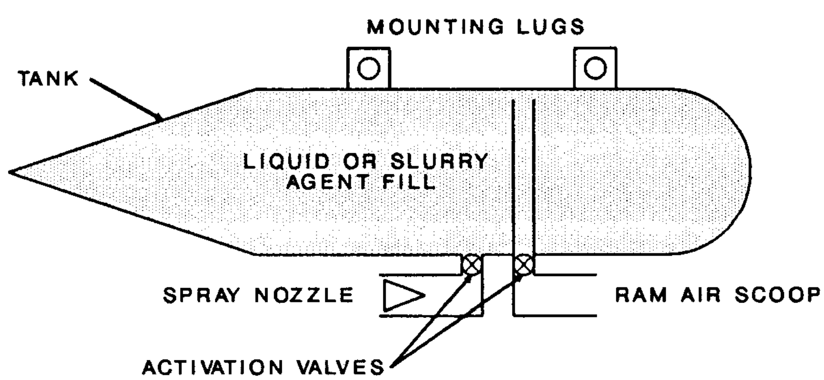
An aircraft spray bomb for delivering binary chemical agents is similar but much more complicated. Figure A-12 shows an aircraft bomb for delivering the binary chemical agent VX. A ballonet (flexible foil balloon) is surrounded by sulfur and inserted into a thin, scored metal cylinder. This cylinder is inserted into a bomb-shaped tank filled with the binary agent QL. When the bomb is released, a gas generator ignites expanding the ballonet. The expansion of the ballonet forces the sulfur to rupture the scored cylinder and be forced into contact with the QL. The gas generator also causes the cylinder (which has small paddles attached to its outer surface) to spin rapidly. The spinning paddles stir the sulfur-QL mixture allowing a chemical reaction to occur which forms VX. After sufficient mixing time has occurred, explosive cutters create holes in the front and rear ends of the projectile. Ram air pressure then causes the VX to spray out of the aft holes, creating a long linear cloud of agent.

Figure A-12. An aircraft bomb for spray cloud dissemination of the binary chemical agent VX.



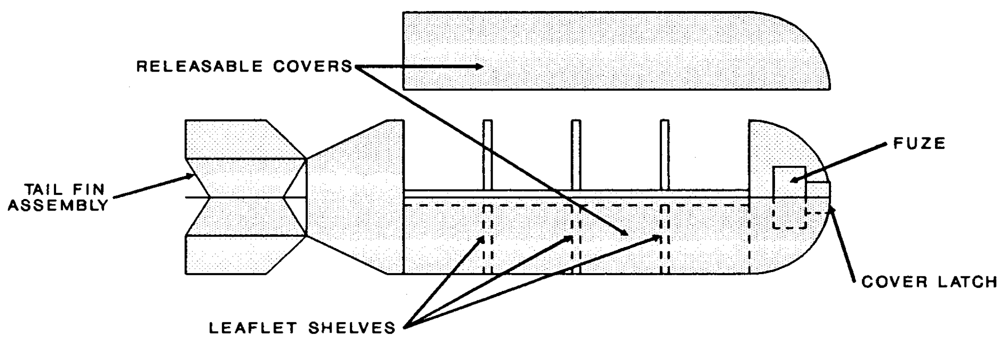
A fixed aircraft spray tank is an alternative to an expendable spray "bomb" in generating a line source of agent. An aerodynamic tank is filled with agent and mounted to an external stores station of the aircraft. The tank can be pressurized by opening a valve connecting the tank to a ram air scoop. After pressurization, opening a second valve will allow the "fluid" agent to be forced through a fine nozzle, which will produce aerosols drops of the desired size. Closing the valves seals the remaining agent in the tank. An aircraft spray tank is illustrated very generically in Figure A-13. These tanks are similar to those used on crop-dusting aircraft. They may also be mounted on high-speed surface vehicles or boats.

Figure A-13. An aircraft spray tank for disseminating CBR agents.



A leaflet bomb (such as the U. S. M16 500-lb leaflet bomb) is illustrated in Figure A-14. Originally designed to scatter leaflets over enemy positions as part of psychological warfare campaigns, the leaflet bomb can be adapted to disseminate some forms of biological agents. The bomb contains several shelves onto which leaflets can be stacked. In biological weapon use, the contents might be feathers, sawdust, or mouse droppings contaminated with a biological agent like anthrax or hantavirus, or they might possibly be chilled, infected insect vectors (such as yellow fever-carrying mosquitoes or encephalitis-carrying ticks). Two releasable half-shells latch together at the front of the "bomb", confine the contents, and provide an aerodynamic shape. The bomb is carried on the aircraft like any other bomb of its size. After release, the fuze, which may be altimetric or timed, releases the cover latches. The covers are torn away from the body by the air stream, exposing the contents of the bomb. These are subsequently scattered over a wide area.

Figure A-14. A psychological warfare leaflet bomb that can be adapted to delivery of "live" biological agents.



Mines (land and naval) are also potential mechanisms for delivering CBR agents. Figure A-15 shows a land mine capable of disseminating CBR agents. A large, usually cylindrical case is filled the agent. A burster charge of explosives is located under the case. A fuze assembly (usually pressure actuated by a footstep, but possibly electrically triggered from a remote site) is added to determine when the mine is to detonate. The whole assembly is either buried with the fuze just below the surface or hidden near ground level using camouflage. When the fuze is triggered, the burster charge explodes, rupturing the case and forcing most of the agent to be pushed up and out from the mine. The agent cloud then settles over a wide area around the location of the mine. Mines of this type could be easily improvised in the field using materials such as grenades, gasoline cans, plastic explosives, and any agent that could be obtained (toxic industrial chemicals or pesticides can be found almost anywhere).

Figure A-15. A nominal land mine for chemical agent dissemination.

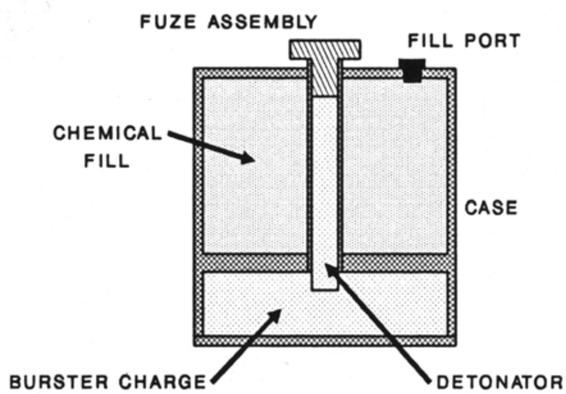


Figure A-16 shows a hypothetical Naval mine for dispersing CBR agents. The mine is moored close to the bottom of shallow water channels (50 to 200 m depth). A multiple influence fuze detects the presence of specific types of warships. When the desired ship class is detected, the mine capsule is released. It rises quickly to the surface. When the capsule breaches the surface, a small powder charge launches a CBR agent-filled projectile a short distance into the air. At the height of its travel (50-100 m altitude), the agent-filled projectile explodes, showering the passing ship with a large cloud (tens to hundreds of kilograms) of agent. The attack occurs so quickly that the ship will likely be contaminated before the ship can be hermetically sealed and collective protection engaged. The agent will be resistant to decontamination with seawater.

Figure A-16. A hypothetical naval mine for attacking ships with CBR agents.

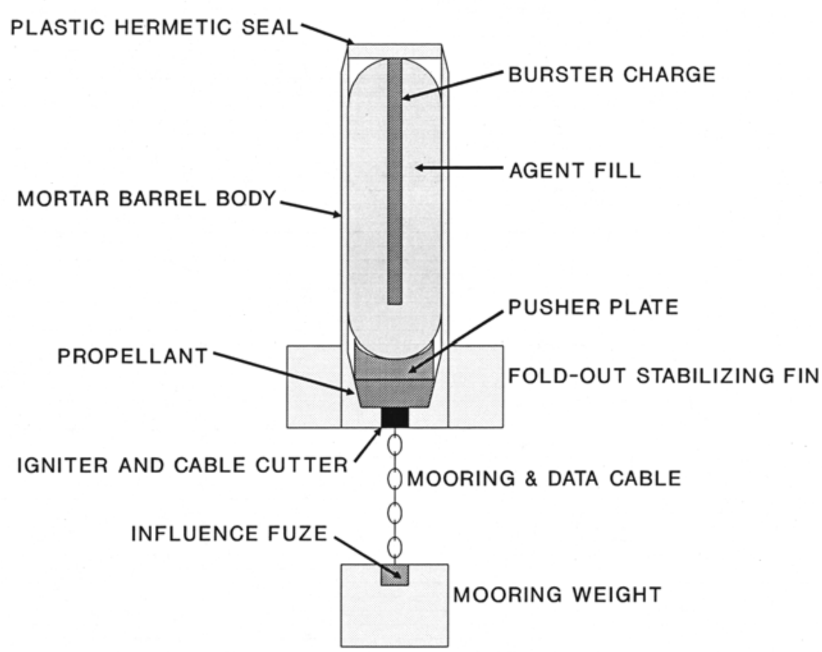
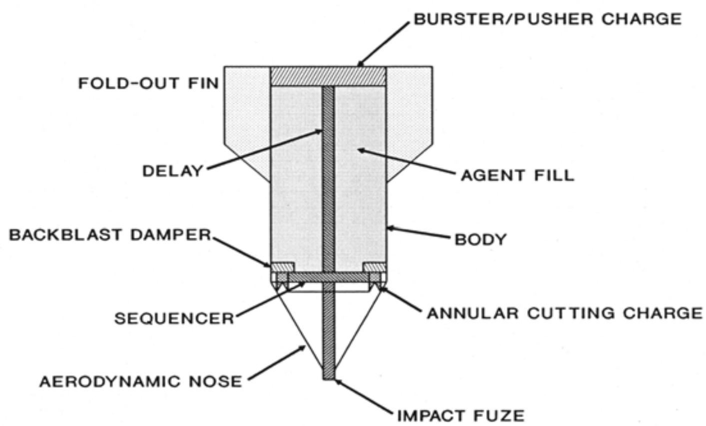


Figure A-17 shows a hypothetical bomblet (submunition) capable of cutting a hole in deck panels to inject its CBR agent contents directly into the interior of a vessel. Such bomblets could defeat the collective protection system of a warship. Such submunitions might be delivered by cruise missiles, ballistic missiles, or aircraft. When the bomblet impacts the deck of a ship, the annular shaped charge fires, cutting a circular hole through the deck into the compartment below. A few milliseconds later, the burster (pusher) charge forces the agent through the hole and disperses it widely throughout the penetrated compartment.

Figure A-17. A hypothetical submunition for injecting CBR agents into the interior of a vessel by punching a hole through the decks and overcoming the collective protection system.



PROLIFERATION OF WMD

If only a few (presumably responsible) nations possessed weapons of mass destruction, and were willing to abide by treaties already in force, then we would have little to worry about, and there would be no need for this appendix. However, dozens of nations, including more than a few irresponsible and even rogue nations, are believed to possess WMD [153]. Table A-3 lists the status of WMD proliferation. Each major class of WMD is listed in a separate column.

There are four categories of "proliferators". **Known** proliferators are those nations for which there is incontrovertible proof (including often their own open admission) that they possess a class of WMD. **Former** proliferators include those states who are known to have possessed a class of WMD (or had a major program to acquire a class of WMD) in the past and who claim to have destroyed that WMD and are believed to no longer possess an offensive WMD program. **Probable** proliferators include those states that are strongly suspected of possessing a WMD capability or of actively attempting to acquire such a capability. It is a virtual certainty that one or more of these probable proliferators actually does possess an offensive WMD capability. **Possible** proliferators include those nations that have caused other nations to suspect that they are attempting to acquire (or have acquired) a WMD capability. Often these states openly possess a defensive WMD research program that could be a cover for a covert offensive WMD program.

A development of major significance to the United States is the growth of both domestic and international terrorism. In the past terrorist groups were content to blow up buildings or hijack airliners. However, in the past few years we have seen several terrorist groups acquire chemical and biological weapons. It is likely that more and more terrorist organizations will attempt to acquire one or more types of WMD. Since many terrorist groups have accepted support from and even allied themselves with potential adversary states, the acquisition of WMD by these groups is something that must be considered when studying the access denial problem. Adversary-sponsored and -directed "terrorist" attacks using WMD against critical infrastructure targets could significantly degrade the U. S. ability to respond to an overseas crisis.

The use of a terrorist group as a surrogate WMD strike force may be viewed as a risk reduction strategy by an adversary. If a terrorist group uses WMD against the U. S., then the supplier state has at least one level of insulation against U. S. retaliation. World opinion will force our government to obtain incontrovertible proof that the adversary intentionally supplied the WMD to the terrorist group before retaliatory action against another sovereign state would be condoned. This evidence may be difficult if not impossible to obtain. If it takes too long to obtain and any other significant factors (such as the leader of the adversary state) change in the intervening time we may be effectively stopped from retaliating. Furthermore, the retaliation will probably not be in kind. If a terrorist group exploded a nuclear device in New York City, the U. S. would be unlikely to vaporize the capital city of the presumed guilty supplier state. More likely the U. S. would destroy some military or industrial target at a time and place that minimized civilian casualties. It is entirely possible that the adversary might view this as an acceptable trade. They might even find it advantageous to continue trading a major U. S. city for a major military facility until the U. S. responded by upping the retaliatory ante.

Table A-3. Proliferation of Weapons of Mass Destruction (WMD)

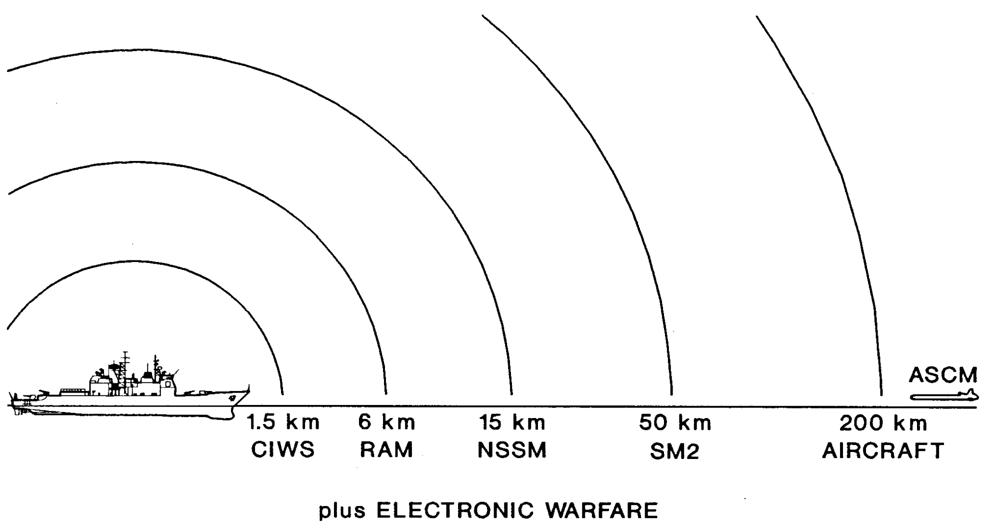
	NUCLEAR	BIOLOGICAL	CHEMICAL	RADIOLOGICAL
KNOWN	China France India Pakistan Russia U. K. U. S.	Iraq Russia	India Iraq Russia U. S. Yugoslavia	None
FORMER	Argentina (R) Belarus Brazil (R) Germany (R) Japan (R) Kazakhstan Romania (R) South Africa Taiwan (R) Ukraine	Canada France Germany Japan South Africa U. K. U. S.	Canada France Germany Italy Japan South Africa U. K.	U. S. (R) Iraq Russia (R)?
PROBABLE	Iran (R) Iraq (R) Israel North Korea	China Iran	China Egypt Ethiopia Iran Israel Libya Myanmar (Burma) North Korea Pakistan South Korea Syria Taiwan	None
POSSIBLE	Algeria (R) Yugoslavia	Algeria (R) Bulgaria Cuba Egypt (R) India (R) Israel (R) Libya (R) North Korea (R) Syria (R) Taiwan (R)	Afghanistan Algeria Cuba Indonesia Laos Sudan Thailand Vietnam	Yugoslavia

(R) denotes a known active research program, but little evidence of weaponization

APPENDIX B. ANALYSIS OF ACTIVE DEFENSE

Historically, surface ships have relied on layered active defenses to defend against cruise missiles [39]. As illustrated in Figure B-1, the layers of defense involved aircraft, long-range missiles, short-range missiles, guns, electronic jammers, and decoys. The total probability of killing an incoming threat is related to the kill probabilities of each layer as shown in the figure. For the decades of the 1970's and 1980's the major threats to warships was assumed to come from cruise missile attacks launched by massed elements of the Soviet Fleet, and/or cruise missile attacks by division-sized bomber elements of Soviet Naval Aviation. Any and all engagements involving our Navy would be blue water (open oceans off of the continental shelves) actions. The maximum credible attack consisted of perhaps 100-200 cruise missiles targeted against a carrier battle group. Carrier-based aviation would engage the surface fleet or bomber forces before those forces could launch their missiles. Shooting the "archer" was preferable to shooting down the "arrows". Invariably, a sizeable number of "archers" would survive the air attack or be able to fire their "arrows" before being shot down. A few dozen missiles would remain for the next layers of defense. Any remaining available carrier aircraft would attempt to shoot down in flight any missiles they could. Long-range Standard missiles (SM-2) would engage the cruise missiles as soon as the AEGIS system (or its Cooperative Engagement Capability upgrade) could detect and track them. At shorter ranges, Sea Sparrow or Rolling Airframe

Figure B-1. Layered defenses against antiship cruise missiles.



$$P_K = 1 - (1-P_{AC})(1-P_{SM2})(1-P_{NSS})(1-P_{RAM})(1-P_{CIWS})(1-P_{EW})$$

Missiles (RAM) would engage those cruise missiles surviving the SM-2 layer. At minimum range, the Phalanx Close-In Weapon System (CIWS) would lay down a barrage of bullets at any target surviving the Sea Sparrow or RAM attacks. All of the preceding layers would be back-stopped by SLQ-32 electronic warfare systems, launching a variety of chaff and infrared decoys, and possibly employing rf jamming. Given the Cold War threats, analysis consistently showed that only a few, if any, missiles or torpedoes would survive to impact our warships. However, we envision a different threat, one with many more missiles. In this case, a dramatically different conclusion will be reached.

This results because a ship or battle group can carry only a finite number of missile kills in its inventory. A typical battle group in 2020 might consist of an aircraft carrier (CVN), one AEGIS cruiser (CG), two AEGIS destroyers (DDG), and three new destroyers (DD-21 class). Let us calculate the number of missile kills such a battle group might possess. The aircraft carrier would have an air wing of 60-80 aircraft. Of these aircraft no more than 36 would typically be assigned to combat air patrol (CAP) missions. Of course, not all of these aircraft would be flightworthy at the same time. Perhaps 10% would be "down" for maintenance. Although only a fraction of the flightworthy aircraft will be airborne unless at least a half-hour of early warning is given, for the purposes of this analysis we will assume all flightworthy CAP aircraft have been sortied. We further assume that each of the roughly 32 carrier aircraft available for CAP might be able to intercept 4 missiles in a massive raid. Four intercepts per aircraft is not the maximum possible. However, air-to-air loadout is likely to be 6 to 8 AMRAAM missiles depending on whether the interceptor is an F-18 or a Joint Strike Fighter (JSF). It is unlikely that every missile will achieve a kill. It is also unlikely that an interceptor aircraft will be able to find, chase down, track, and attack more than four or five small, high-speed missiles in the 4-6 minutes that it takes the incoming missiles to close from a nominal 300-km aircraft patrol outer envelope to within SM-2 missile range. Once SM-2 missiles can be brought to bear on the threats, the interceptors must break off the fight or risk being inadvertently shot down by our own missiles. All factors considered, 4 intercepts per aircraft is optimistic. Thus, CAP may account for as many as 128 missile kills.

Among the surface combatants, there may be as many as {0 (CVN) + 128 (CG) + 96 (DDG) + 96 (DDG) + 128 (DD) + 128 (DD) + 128 DD)} = 704 VLS cells [59]. Two-thirds of the AEGIS ship cells may contain Standard Missile SM-2 (214 total) and 1/8 of the DD-21 cells may contain four-packs of Sea Sparrow missiles (192 total) for air defense. This is not an unreasonable loadout given that the AEGIS ships are primarily air dominance ships and the DD-21's are primarily land attack ships. Many of the total VLS cells must be devoted to Tomahawk (land attack) and antisubmarine warfare missions. If any of the ships has an exoatmospheric ballistic missile defense mission, then even fewer VLS cells will be available to carry SM-2s or Sea Sparrows. In addition to all of the missiles, the battle group may have (4 + 2 + 2 + 2 + 2 + 2 + 2) = 16 CIWS Gatling guns, each good for roughly 4 kills each under ideal conditions. A CIWS carries roughly 1500 rounds of ammunition good for approx. 30 seconds of firing at the nominal 3000 round per minute rate. The maximum range of the CIWS rounds is about 6000 m with a quoted effective of about 1500 m. Continuous firing at an incoming subsonic missile over the range from 2500 m to 500 m (approx. 6.7 seconds) will almost certainly (but not always) result in a kill. Continued firing at targets closer than 500 m will increase the hit probability, but the probably of receiving serious damage from missile debris rises rapidly as the destruction range decreases below 500 m. In any event CIWS is capable of only four complete 6.7 second bursts before requiring rearming. Any engagement for shorter times will have an increased probability of miss. Thus, assigning 4 kills per CIWS is optimistic. The electronic warfare systems will contain a mix of some systems with passive detection, active jamming, and chaff/flare dispensers and some systems without active jamming capability. Systems with jamming will be somewhat more effective against rf-guided missile than systems employing only chaff. Both will have the same limited effectiveness against ir-guided missiles. All things considered, the EW systems may be expected to negate roughly half of those missiles that are not destroyed by the hard-kill defenses.

Assume that the antimissile missiles are 95% reliable and effective (historically very good performance – many missiles do not perform this well) and that only one missile is launched at each threat. Also assume that the aircraft and CIWS systems are 100% effective at achieving their stated number of kills. Then the battle group is capable of killing at most 128 + {0.95 x (214 + 192)} + 64 = 578 hard kills with soft kills on half of the remaining threat. The NPS Red Team results suggested that 1000 missiles per attack (2-3% of a near peer competitor's inventory and 10-20% of a regional competitor's inventory) was not an unreasonably large expenditure for attacking (and almost certainly destroying) a battle group. In this instance, assuming that only 80% of the launched threats functioned properly, then 111 missiles would survive to hit the 7 ships of the battle group (16 hits per ship). If each CIWS were replaced by an 11-missile Sea-RAM launcher (providing roughly 103 <u>additional</u> hard kills per battle group), then 60 missiles would survive to hit the 7 ships (giving 8-9 hits per ship).

In practice, several factors would make the actual numbers of hits per ship even larger. Temporal saturation of the defenses due to finite defensive engagement rates will permit some cruise missiles to close to zero range without ever being attacked. A traditional shoot-shoot-look-shoot firing doctrine, selected to optimize the number of kills in an engagement rate-limited system, causes two missiles to be fired at each missile threat to increase the kill probability. This will deplete the missile magazines twice as quickly. This will also make temporal saturation of the defense easier to achieve. Despite wishes and best intentions, some cruise missiles will escape being killed by the missiles fired at them. Additional missiles must be fired at those threats that were missed by the first shots, further depleting the magazines. If the incoming raid contains a very large number of missiles, it will be difficult to allocate a single shooter against each missile. To the extent that command and control discipline breaks down and two or more different ships fire on exactly the same missile threat, then missiles will be wasted and magazine depletion will occur even faster. As an additional complication, the attacking missiles will not be uniformly distributed against the targets. It is quite likely that the majority of the attacking missiles will concentrate on the largest targets (the carrier and the AEGIS cruiser). Even though this may not increase the total number of leakers, it means that if there are a total of 111 leakers, then the larger ships might take 30, 40, or even more hits apiece rather than only 16.

For these and other reasons a single massive strike is probably not the best enemy strategy. A smaller but still massive first strike (of say 500 missiles) would be followed by damage assessment and a subsequent smaller second strike to finish off survivors would permit the adversary to conserve more of his resources. Variations with several sequential strikes might permit as few as 500 missiles to completely destroy a battle group. It should be noted that complete destruction means just that. Given our ships' current questionable ability to take even a single hit and then continue fighting, it is likely that raids even smaller than 500 missiles would eliminate a battle group as an effective force.

Doubling the size of the defensive suite might effectively counter a 1000-missile raid but would also add enormously to the cost. Payload costs would roughly double and each ship would have to get substantially larger to handle the increased number of missile launch cells. More launch cells are necessary because removal of the land attack, ballistic missile defense, and antisubmarine missiles currently assumed to be loaded in the remaining VLS cells to make room for additional air defense missiles, will prevent the battle group from performing its primary missions. Total battle group cost would likely increase by 30-50%. Of course, even this doubled defense could be defeated by 1500-missile attacks. It will cost the adversary far less to buy more missiles and launchers/launch platforms than it will cost us to put more defensive weaponry on each of our ships. Buying twice the number of combatants is of course totally out of the question from a cost perspective. Even if the Navy was able to mount a task force with all 12 of its carrier battle groups, a 12,000 missile attack is not beyond the capability of a peer competitor and might deplete less than a third of that competitor's anticipated missile inventory. The fleet-wide integration of the Cooperative Engagement Capability [40] will allow optimum use of the available weaponry, but will not affect the outcome – all the defensive weapons are used up before the incoming raid can be depleted of missiles.

The trade between offensive weapon costs and defensive weapon costs gets even worse in the littorals. If the Navy is close enough to bombard targets on shore, weapons on shore are close enough to bombard the Navy. In addition to cruise missiles, land-based artillery [43]-[45] (possibly with imaging seekers on maneuverable projectiles), aircraft (including civilian aircraft with improvised armaments, armed drones, and kamikazes – manned by martyrs or remotely-piloted), and small anti-armor weapons fired from "non-combatant" vessels such as small fishing boats, must be considered.

APPENDIX C. MISSILE NOMENCLATURE

Missiles come in many varieties and can be sorted into many different categories. One categorization is based on the locations of the launch platform and the target. For example, an air-to-air missile (AAM) is air-launched at an airborne target. Other categories include: surface-to-air missiles (SAM), surface-to-surface missiles (SSM), and air-to-surface missiles (ASM – although this abbreviation usually stands for anti-ship missile) or air-to-ground missiles (AGM). Another categorization is guided versus unguided. Unguided "missiles" are usually referred to simply as rockets. Rockets follow a simple trajectory governed at first by the propulsion characteristics, and later follow a ballistic trajectory after the rocket motor burns out. Most military missiles are guided. One major classification of guided missiles is based on guidance type.

Inertially-guided missiles measure the linear and angular accelerations to which the missile is subjected. Position is determined by double integration of the linear accelerations (as measured in inertial coordinates). An autopilot commands the missile to fly a preset course with respect to inertial coordinates. This course may be as simple as a straight line determined by the initial axis of the missile (some very short-range anti-armor weapons employ this trajectory). It may also be a more complicated course that ends up at motor burnout with the missile at a specific point in space, traveling with a specific velocity (remember that velocity is a vector quantity; speed is a scalar). When subsequently acted on by gravity and other environmental forces, the missile will follow a ballistic trajectory that impacts near the intended target.

Inertial guidance is a form of "navigational" guidance, or guidance by knowing where the missile and the target are in space. Two other forms of navigational guidance are commonly employed. If the missile possesses a Global Positioning System (GPS) receiver, then it can determine exactly where it is in earth-centered coordinates. The missile is given a set of coordinates where the target is located and the autopilot flies a course that ultimately brings the missile GPS location into coincidence with the target GPS location. If the missile possesses an altimeter, it may be possible to utilize terrain contour matching (TERCOM) guidance. The missile carries a number of small topographic "maps" in its computer memory. While in a segment of level flight near a planned checkpoint, the missile measures the altitude profile of the ground beneath it. This terrain height profile is correlated against one of the stored topographic maps to determine which segment of the map matches the observation. Once a match has been determined, the missile knows its location and its direction of motion. It is then a simple command to give it a new heading to take it to the next checkpoint.

Command-guided missiles require a fire control sensor that tracks both the target and missile, a computer that calculates missile course adjustments necessary for intercept, and a communication link to communicate those course adjustments to the missile. The fire control sensor may be a radar or an electro-optical sensor. Some newer variants of command-guided missiles place an imaging sensor on the missile with a two-way communication link. The operator detects the target via the sensor image and gives up-down/left-right commands to the missile to keep the target in the center of the sensor image.

Homing missiles have seekers that detect the position of the target with respect to the direction of missile motion and compute guidance commands that permit the missile to ultimately impact the target. Homing seekers may be active (radiating energy from the seeker and detecting energy backscattered from the target), semi-active (detecting energy backscattered from the target produced by illumination from a separate radiating aperture – often back at the launcher), and passive (detecting energy emitted by the target). Active seekers usually employ small radars for radiation and detection). Semi-active seekers may operate at microwave frequencies or laser frequencies. The latter are called laser-guided missiles. Passive seekers may detect microwave emissions or infrared emissions. Missiles employing the former are called anti-radiation homing missiles; the latter are called infrared-guided missiles.

Three classification schemes involve the propulsion mechanism. If both the fuel and the oxidizer (a fuel combines chemically with an oxidizer in a process called combustion) are carried on board the missile, the missile uses rocket propulsion. If the missile carries only fuel and draws in external air as the oxidizer, the missile uses air-breathing (or jet) propulsion. A missile that has a single motor (or cluster of motors that burn simultaneously) it is said to be a single-stage missile. If the missile has two or more motors that burn one after the other and each earlier motor is discarded as soon as it burns out it is said to be a multi-stage missile. A stage whose function is to produce rapid acceleration of the missile is called a booster. A stage whose function is to barely overcome the velocity-reducing effects of atmospheric drag and gravity is called a sustainer. Boost-sustain is a common two-stage missile configuration. The booster motor accelerates the missile from zero to maximum speed; the sustainer motor keeps the missile flying near its maximum speed. Many anti-aircraft missiles use a boost-sustain configuration. Missiles that use only (one or more) booster rocket stages are commonly called ballistic missiles. Missiles that use a sustainer stage for all but the initial portion of the flight and are capable of flying relatively long distances are called cruise missiles. Many cruise missiles use air-breathing propulsion in the sustainer motor.

Cruise missiles can be further classified by the trajectories they fly and the targets they are capable of striking. Cruise missiles that fly at low altitudes over water (a few meters to less than or equal to 30 meters) are called sea-skimming missiles. Some missiles fly at high altitudes (drag and aerodynamic heating are reduced at high altitudes) and dive at steep angles (approaching 45°) towards the target after target detection. These are often referred to as "high divers". Some missiles fly at low altitudes until they come within an estimated short distance of the target location, at which time they "pop up" to a modest altitude, search and detect the target, and then either dive at the target or return to "sea skimming" altitude until impact. Cruise missiles with the ability to independently find a moving target are used as "anti-ship" cruise missiles. Anti-ship cruise missiles invariably have active or passive seekers. Cruise missiles that can accurately guide to a known point in inertial space are used as "land attack" cruise missiles. Most land attack cruise missiles use navigation guidance (inertial, GPS, or TERCOM) guidance.

There is no standard terminology for describing ballistic missiles with different maximum ranges. The terminology used by the author is given below. For comparison the author has listed the terminology used in the Intermediate Nuclear Forces (INF) Treaty [154] and the Anti-Ballistic Missile (ABM) Treaty [21].

Author	*Range*	*INF Treaty*	*ABM Treaty*
Short-range	*< 500 km*	*---*	*---*
Medium-range	*500 – 1000 km*	*Shorter-range*	*---*
Intermediate-range	*1000 – 3500 km*	*Intermediate-range*	*---*
Long-range	*3500 – 5500 km*	*Intermediate-range*	*"No tests against"*
Intercontinental	*> 5500 km*	*---*	*"No tests against"*

"No tests against" means that missiles of these ranges may not be used as targets for testing any missile defense system except the one treaty-authorized "ABM system". Note that the author's usage encompasses all of the different breakpoints used by the two treaties. The National Air Intelligence Center [155] uses similar labels but a different set of breakpoints:

NAIC	*Range*
Short-range	*< 1000 km*
Medium-range	*1000 – 3000 km*
Intermediate-range	*3000 – 5500 km*
Intercontinental	*> 5500 km*

The NAIC breakpoints are not consistent with the treaty language. The Center for Defence and International Security Studies in the United Kingdom promulgates the following classification scheme.[258]

CDISS	*Range*
Battlefield Short Range	*< 150 km*
Short Range	*150 – 800 km*
Medium Range	*800 – 2400 km*
Intermediate Range	*2400 – 5500 km*
Intercontinental Range	*> 5500 km*

The former Soviet and now Russian military uses a different nomenclature scheme for their missiles.[259]

Russian	*Range*
Tactical	*< 50 km*
Operational-Tactical	*50 – 300 km*
Operational	*300 – 500 km*
Operational-Strategic	*500 – 1000 km*
Strategic	*> 1000 km*

APPENDIX D. BALLISTIC MISSILE DEFENSE

There are a variety of conceptual systems for defense against ballistic missiles. The systems may be ground-based, airborne, or space-based. The kill mechanism may involve directed energy (destruction by high-energy lasers) or kinetic energy (destruction through direct high-speed impact of a "kill vehicle" with the missile). Kinetic energy kill is possible at high relative velocities. Assuming the incoming target to be much, much more massive than the kill vehicle, we may assume that the center of mass of the combined target interceptor system is roughly coincident with the target center of mass. Since incoming missiles typically have masses of several thousand kilograms and kill vehicles typically have masses of the order of 50 kg or less, the center of mass approximation above will cause very small errors in any calculation. If m is the mass of the kill vehicle and V is the relative velocity between the target and the kill vehicle, then the kinetic energy E potentially released in the impact is roughly

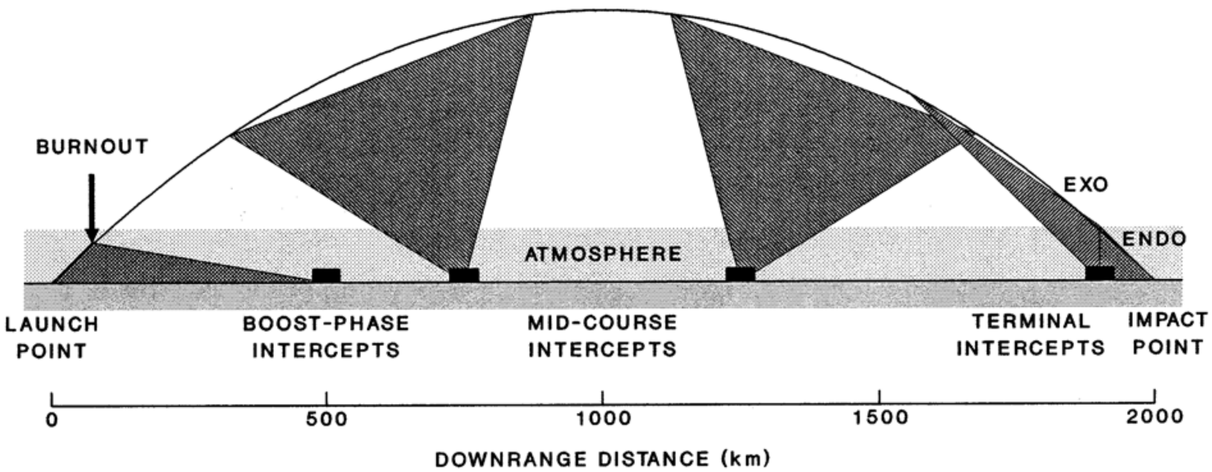
$$E = 0.5\, m\, V^2.$$

Let us assume an incoming target velocity of 2000 m/s, an outgoing kill vehicle velocity of 2000 m/s (yielding a relative velocity of 4000 m/s), and a kill vehicle mass of 50 kg, then for a direct hit, the kinetic energy released is 4×10^8 Joules. In an impact, the kinetic energy will be transformed into heat energy. By way of comparison, explosion of 1 kg of TNT releases 4.2×10^6 Joules, mostly as heat energy. Thus our hypothetical kinetic energy intercept releases as much energy as 100 kg of TNT, more than enough to completely destroy both target and kill vehicle.

Intercept (or destruction) can occur within the atmosphere (endoatmospheric – altitudes nominally less than 100 km) or above the atmosphere (exoatmospheric – altitudes nominally greater than 100 km). It may occur during any of the phases of missile flight, as illustrated in Figure D-1. Boost phase intercepts occur while the ballistic missile's rocket motors are still firing. Post-boost phase intercepts occur while a post-boost vehicle (PBV), if any, separates from the missile body and dispenses one or more reentry vehicles (RV) and/or penetration aids (penaids or decoys). PBVs are usually associated with Multiple Independently-targeted Reentry Vehicles (MIRVed) ballistic missiles. Mid-course intercepts occur after the post-boost phase (if any) and before terminal phase. Terminal phase intercepts occur as the RV (in some cases the entire missile) begins to reenter the atmosphere. Defense systems may provide defense of an extended region (area defense) or they may provide defense of a very limited area centered on the defense system (point defense). Area defense systems may provide only rear area defense (the defense system is positioned between the ballistic missile launch site & the defended area) or general area defense (the defended area includes the defense system position). General area defense systems are capable of point defense; rear area defense systems are not.

Figure D-1 specifically illustrates the trajectory of a 2000 km range missile. The ranges of potential intercepts for a nominal 500 km range interceptor (or directed energy weapon for boost phase intercepts) at several ground positions along the missile trajectory are illustrated by the shaded triangular regions. The reader should note that an interceptor fast enough to intercept

Figure D-1. Ballistic missile defense geometries.



another missile at 500 km range is a very large missile in its own right (much larger than tradition long-range air defense missiles).

Complete ballistic missile defense systems have a number of components. For every kind of system there must be a warning element that detects the launch of a missile or the mid-course flight of a reentry vehicle and cues the defense system. There must also be a tracking system that reacquires the incoming target and determines where and when to point a directed energy weapon or fire an interceptor missile. Additional components of a directed energy weapon system are described in Appendix I. For the remainder of the present appendix we will consider only kinetic energy weapon systems. Kinetic energy weapon systems further require a launcher and an interceptor. The interceptor typically consists of one or more booster stages and a kill vehicle. The kill vehicle contains a homing seeker (typically active radar or passive infrared) and a guidance & control system consisting of attitude control motors and divert thrust motors. The divert system produces thrust directed through the kill vehicle center of mass. Thus it produces pure lateral motions that can be used to steer the kill vehicle into the path of the incoming target. The kill vehicle may also have a "kick motor" oriented back along the direction of motion to provide additional acceleration and velocity at intercept. The higher the relative velocity, the higher the kinetic energy released at impact.

For purposes of this paper it is useful to "quantify" some of the characteristics of kinetic energy defense systems. Rear area defense against intermediate-range ballistic missiles is somewhat easier than point defense. In rear area defense, intercepts are made while the missile passes overhead the shooter. "Overhead" is used loosely. In general, the interceptor travels more vertical distance than horizontal ground track distance. Detection occurs along a line of sight that makes a significant angle to the interceptor trajectory. In point defense, the geometry is more or less nose-on. Detection occurs along the same line of sight as the interceptor trajectory. For an intercept at a given high altitude, the average target velocity will be essentially the same for both area defense and point defense intercepts. If we assume the same interceptor velocity in both cases, then the angle, A, between the interceptor velocity vector and the target velocity vector is $A(pd) \approx 180°$ for point defense, but $A(ad) << 180°$ for area defense. Then from the law of cosines

$$(a^2 = b^2 + c^2 - 2bc\ cosA)$$

where a, b, and c are the sides of the triangle, and A is the angle opposite side a, it is obvious that a (the minimum detection range) is substantially larger for point defense than for area defense, when b is associated with the distance the target moves before intercept and c is associated with the distance the interceptor flies out before intercept.

If intercepts are allowed within the atmosphere, then the target leg of the triangle becomes very small, and the difference in detection range can become negligible. Point defense and area defense become roughly equally difficult. Unfortunately, at velocities exceeding 2 km/s within the atmosphere, it is exceedingly difficult to use a high-resolution imaging seeker, because the aerodynamic heating of the window material (and the air in front of the window) will produce noise that would obscure the target. To guarantee an intercept against a "maneuvering" target, the interceptor velocity must be comparable to the target velocity. Thus, endoatmospheric intercepts are difficult against targets with velocities in excess of 2 km/s (or ranges in excess of 400 km – see below). Exoatmospheric point defense is further complicated by differences in radar cross section of the target. The cross section of a cone (typical reentry vehicle shape) or cone-cylinder (typical missile shape) is at a minimum when viewed nose-on (see Appendix E). The cross section increases rapidly until the viewing angle is perpendicular to the side of the cone (i.e., "broadside" to the cone). For cones, the cross section then falls off again with increasing viewing angle; for cone-cylinders, the cross section continues to increase until the viewing angle reaches 90° (broadside to the cylinder). Thus, in point defense, not only is the range longer, but the radar cross section is smaller, making detection and tracking much more difficult than in area defense.

If some cueing sensor other than the shooter's radar can provide the accurate track data needed to launch the interceptor much earlier in time (than required for a minimum range intercept), then the missile defense system can readily provide both point defense and wide area defense capabilities. Such a cueing sensor might be surface-based (e.g., an AEGIS ship in another battle group closer to the launch point), although more likely it would be airborne or space-based. For example, it is virtually certain that the sensors onboard the Air Force's Airborne Laser could detect and track some targets at ranges well in excess of those at which the laser was capable of engaging those targets. If available, any accurate track data could be provided to the shooter over the Cooperative Engagement Capability.

The maximum range, R, versus total velocity, v, for a ballistic missile is given approximately by the relation

$$R \simeq v^2/g,$$

where g is the acceleration of gravity. In arriving at this simple relation (based on a simple parabolic trajectory) we have ignored the finite time extent of the boost phase, the curvature of the earth, air resistance, and the rotation of the earth. The primary conclusion from this equation – longer-range missiles must have higher velocities – is true even if we had considered the factors we ignored. The velocity of a 1000 km range missile is 41% higher than the velocity of a 500 km range missile. The peak altitude, h, of a maximum range missile is approximately

$$h \cong v^2/4g \cong R/4.$$

The length of time that the missile is within the atmosphere (below 70-90 km altitude) will decrease approximately inversely as the velocity increases. The time of flight from launch to impact, T, is approximately

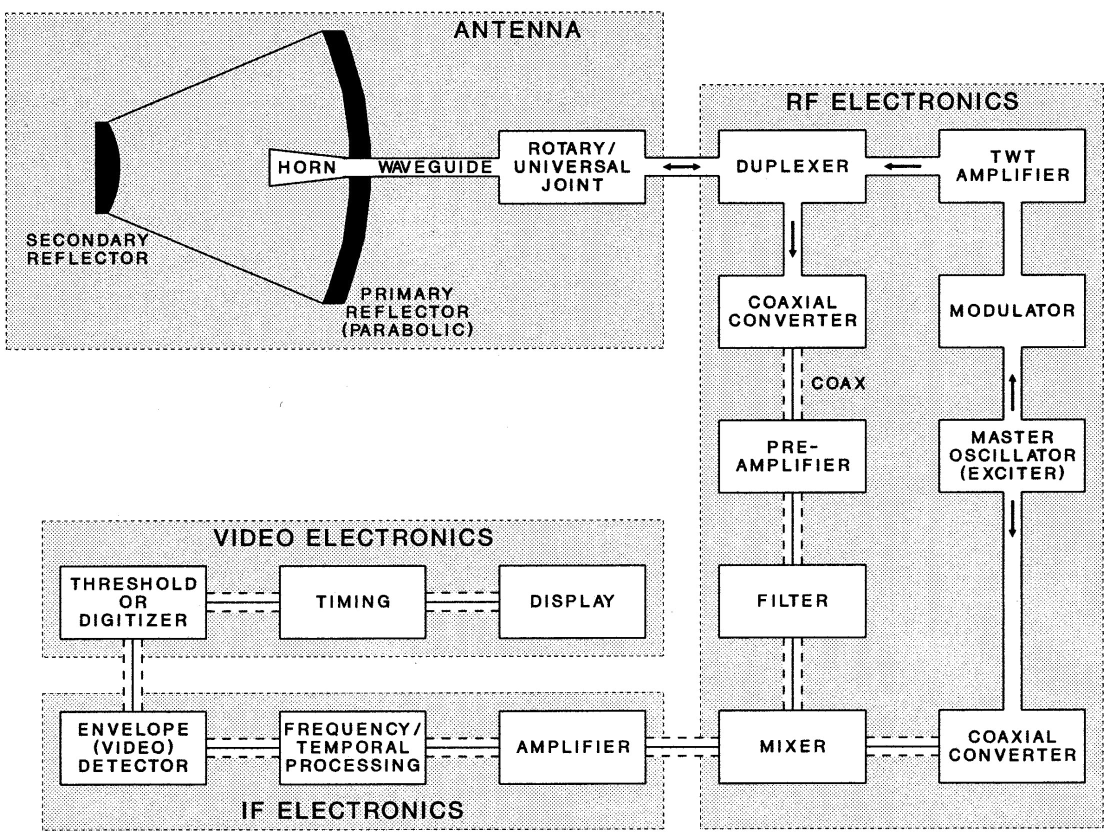
$$T \cong (v\sqrt{2})/g.$$

Thus, a 1000 km range missile will have a velocity of 3.2 km/s, reach an altitude of 250 km, and have a flight time of 450 s. A 4000 km range missile will have a velocity of about 6 km/s, reach an altitude of 1000 km, and have a flight time of 900 s. Note that the approximate relations given above will overestimate the velocity required for an ICBM ($R \geq 15{,}000$ km) by roughly a factor of two. The overestimate for a 4000 km range missile should be about 20%.

APPENDIX E. RADAR PERFORMANCE ESTIMATION

Radars work by transmitting microwave electromagnetic radiation from an antenna towards a target [156]-[157]. The target in turn scatters some of the incident radiation back towards the radar. The radar then collects this radiation with an antenna and mixes it with radiation from a local oscillator in its receiver. The signal coming out of the receiver is finally analyzed to determine the presence of a target, the range or velocity of a target, or some other target attributes. A generic block diagram of a microwave radar is shown in Figure E-1. This diagram shows the arrangement and interconnections of the critical components. It should be noted that alternative technologies may be employed for almost every element. For example, a parabolic dish antenna is illustrated, but this may be replaced by a phased array antenna. A klystron amplifier may be used in place of a traveling wave tube amplifier. Several stages of mixing may be employed rather than the single stage shown. The display may be replaced by an automatic tracker or the input to a missile autopilot. Coaxial cables may replace waveguides and microwave striplines may replace coaxial cables. And so on.

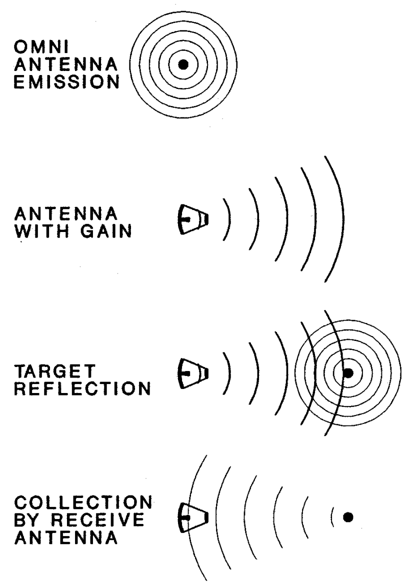
Figure E-1. Block diagram of a generic microwave radar.



The performance of a noise-limited radar is given by the classical radar equation. This expression relates the carrier (average signal level)-to-noise ration *CNR* of the radar to radar parameters (such as power, aperture size, frequency, bandwidth), target parameters (cross section), and propagation parameters (atmospheric losses). Figure E-2 shows a simple graphical derivation of the radar equation. The process used in the derivation is an example of radiometric analysis.

Figure E-2. Derivation of the radar equation.

POWER RADIATED BY RADAR TRANSMITTER	$= P_T$
POWER DENSITY AT RANGE R FROM AN OMNIDIRECTIONAL ANTENNA (α = ATMOSPHERIC EXTINCTION)	$= P_T e^{-\alpha R}/4\pi R^2$
POWER DENSITY FROM A DIRECTIONAL ANTENNA WITH ANTENNA GAIN G_T ($= 4\pi A_T/\lambda^2$; A_T = ANTENNA AREA; λ = RADAR WAVELENGTH)	$= P_T G_T e^{-\alpha R}/4\pi R^2$
POWER INTERCEPTED BY TARGET AND RERADIATED TOWARD RADAR RECEIVER (σ = RADAR CROSS SECTION OF TARGET)	$= P_T G_T \sigma e^{-\alpha R}/4\pi R^2$
POWER DENSITY AT RADAR RECEIVE ANTENNA	$= P_T G_T \sigma e^{-2\alpha R}/(4\pi R^2)^2$
SIGNAL POWER COLLECTED BY ANTENNA OF AREA A_R	$= P_T G_T A_R \sigma e^{-2\alpha R}/(4\pi R^2)^2$
IF RECEIVE ANTENNA AREA IS EQUAL TO TRANSMIT ANTENNA AREA (USUALLY TRUE)	$= P_T A_T^2 \sigma e^{-2\alpha R}/4\pi \lambda^2 R^4$
NOISE LEVEL IN RECEIVER (B = RECEIVER NOISE BANDWIDTH; T = ELECTRONICS TEMPERATURE; F = AMPLIFIER NOISE FIGURE)	$= kTBF$
RADAR CARRIER-TO-NOISE RATIO	$CNR = \dfrac{P_T A_T^2 \sigma e^{-2\alpha R}}{4\pi kTBF\lambda^2 R^4}$



In slightly modified form (the average power divided by the pulse repetition frequency replaces the peak power divided by the bandwidth and the antenna area is replaced by the appropriate expression involving the antenna diameter), the radar equation becomes

$$CNR = P_{AV}\, \pi D^4\, \sigma\, e^{-2\alpha R} / 64\, k\, T\, PRF\, F\, \lambda^2\, R^4$$

where the parameters are defined in Table E-1 below along with numerical values characteristic of three different radar applications.

Table E-1. Parameters of microwave radars used in three generic applications.

PARAMETER	BMD RADAR	MISSILE SEEKER	AD/CMD RADAR
CNR = Carrier-to-Noise Ratio (Required to give desired detection performance)	14 dB	23 dB	33 dB
P_D = Detection Probability	0.9	0.9	0.99
P_F = False Alarm Probability	10^{-8}	10^{-8}	10^{-8}
P_{AV} = Average Transmitter Power	10,000 W	10 W	1000 W
D = Aperture Diameter	16 m	20 cm	4 m
σ = Target Cross Section	0.01 m^2	10,000 m^2	0.02 m^2
Cross Section Statistics	Swerling 0	Swerling 2	Swerling 2
α = Atmospheric Attenuation (Often neglected)	0	0	0
T = Electronics Temperature	300 K	300 K	300 K
PRF = Pulse Repetition Frequency	150 Hz	5 kHz	1 kHz
F = Amplifier Noise Factor (Typically 3 to 10)	10	10	10
λ = Radar Wavelength	5 cm	2 cm	6 cm
f = Radar Frequency	6 GHz	15 GHz	5 GHz
R = Radar Range	950 km	26 km	30 km

There are other parameters of interest in determining radar performance. The Round-Trip Time Delay of the transmitted waveform is

$$t_R = 2R/c.$$

The Ambiguous Range (the maximum target range at which close-in small targets can be differentiated in range from large distant targets – caused by transmitting the next radar pulse before the first pulse's target reflection from a distant target can return to the radar) is given by

$$R_{AMB} = c/2\,PRF$$

where PRF is the pulse repetition frequency. The Doppler shift of a received waveform can be determined from the relation

$$\Delta f = (2V/c) = 2V/\lambda$$

where V is the relative radial velocity (line-of-sight closure velocity). The 3-dB beamwidth of the transmitted beam is roughly

$$\theta_B = 1.045\ \lambda/D$$

while the angular resolution of the radar is approximately

$$\Delta\theta = 0.88\ \lambda/D.$$

The range resolution of the radar may be determined from

$$\Delta R = c\tau/2 = cB/2$$

where τ is the radar pulsewidth and B is the bandwidth of the radar waveform. The choice of resolution expression is governed by whether the radar transmits simple pulses or more complex waveforms. Velocity resolution of the radar may be estimated from the relation

$$\Delta V = \lambda/2\tau = \lambda B/2$$

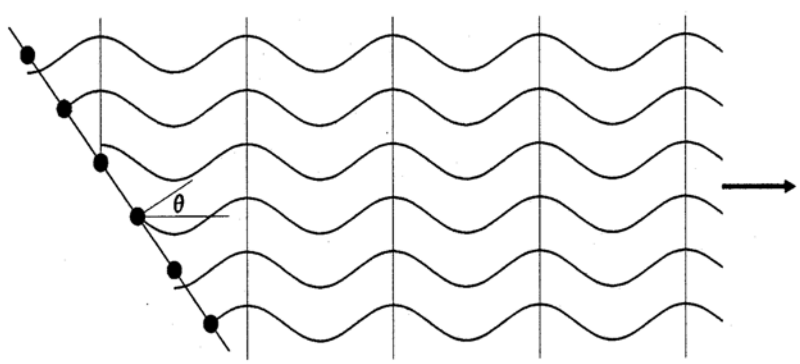
Again the choice of expression depends on the radar waveform. In the radar range equation, peak power P_{PK} or pulse energy E_P may be substituted for the average power by using the equivalence relations

$$P_{AV}/PRF = P_{PK}/B = \tau P_{PK} = E_P\,.$$

The alternative forms of the radar range equation may be easier to use for some calculations.

As mentioned in the first paragraph of this appendix, conventional parabolic antennas are often replaced by phased array antennas. The fundamental principle of phased array antennas is shown in Figure E-3. Consider a regular array of emitters. If there is a regular variation of phase from element to element, then the radiation emitted from each element will be perfectly in phase with the radiation emitted from each other element **in one direction only** (angle θ). This is the direction of radiation emission of the phased array. If the regular variation of phase is altered

Figure E-3. Alignment of emitted wavefronts in a phased array antenna.

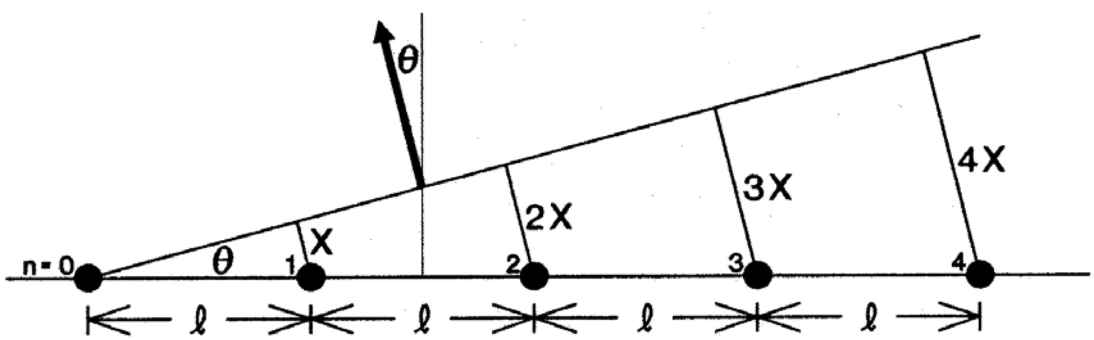


slightly, then the direction of emission will also vary. The regular phase relationship can be determined from Figure E-4. For emitters with spacing *l* and radiation of wavelength λ, the phase of the n^{th} element relative to the zeroth element, ϕ_n, at emission angle θ can be shown by geometry to be

$$\phi_n = n2\pi X/\lambda = n2\pi\,(l/\lambda)\,\sin\theta$$

By applying the phase ϕ_n to emitter element n, the antenna radiation will be emitted in direction θ. This one dimensional result is easily extended to two-dimensional arrays (replace θ by an orthogonal angle β and ϕ_n by a phase variation χ_m in the second array dimension).

Figure E-4. Geometry of phase variation.



The detection probability, false alarm probability, and carrier-to-noise ratio (*CNR* where *CNR = [Mean Received Signal]/[Mean Receiver Noise]*) are interrelated by receiver operating characteristics. The receiver operating characteristics depend on the noise in the receiver, the statistics of fluctuations in the radar cross section, and the statistics of fluctuations in the effective extinction of the propagation medium. Figure E-5 shows the receiver operating characteristic of a conventional microwave radar for a non-fluctuating target. Figure E-6 shows the receiver operating characteristic of a conventional microwave radar for a target exhibiting Rayleigh cross section statistics. Such statistics result when the target can be modeled as the sum of many small, randomly phased scattering centers (Model 2 developed by Swerling). This is often used as a worst case cross section assumption. It is also encountered as a good approximation to the true cross section statistics in a number of examples. The *CNR* values shown in the table above were derived from these receiver operating characteristics.

Calculation of radar cross sections of real objects is complicated. However, simple geometric shapes can be analyzed explicitly. For example, the radar cross section of a smooth metallic sphere of radius *a* and reflectivity ρ is given by

$$\sigma_{sphere} = \pi a^2 \rho \,.$$

Figure E-5. Receiver operating characteristic for a non-fluctuating target.

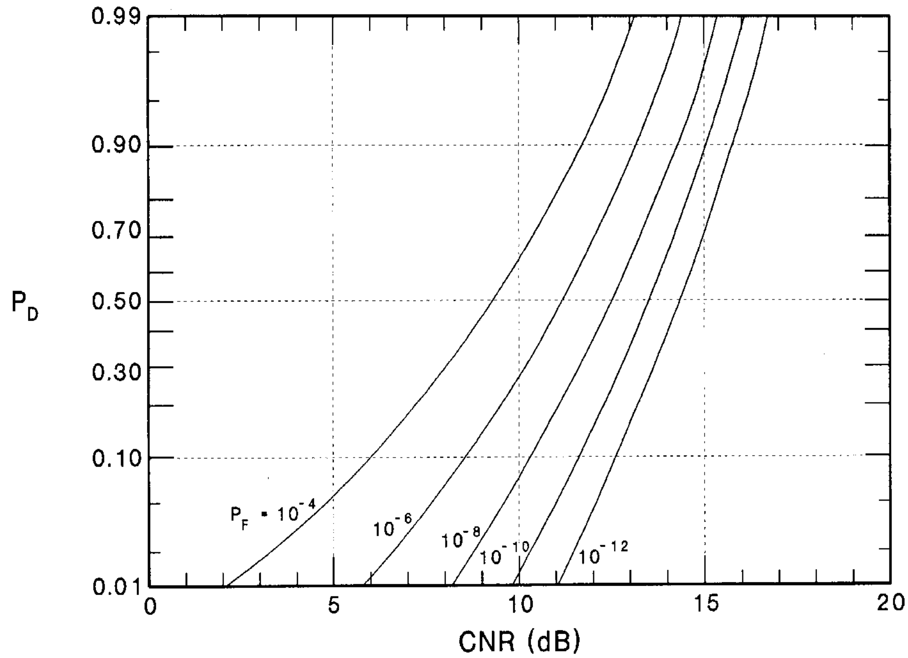
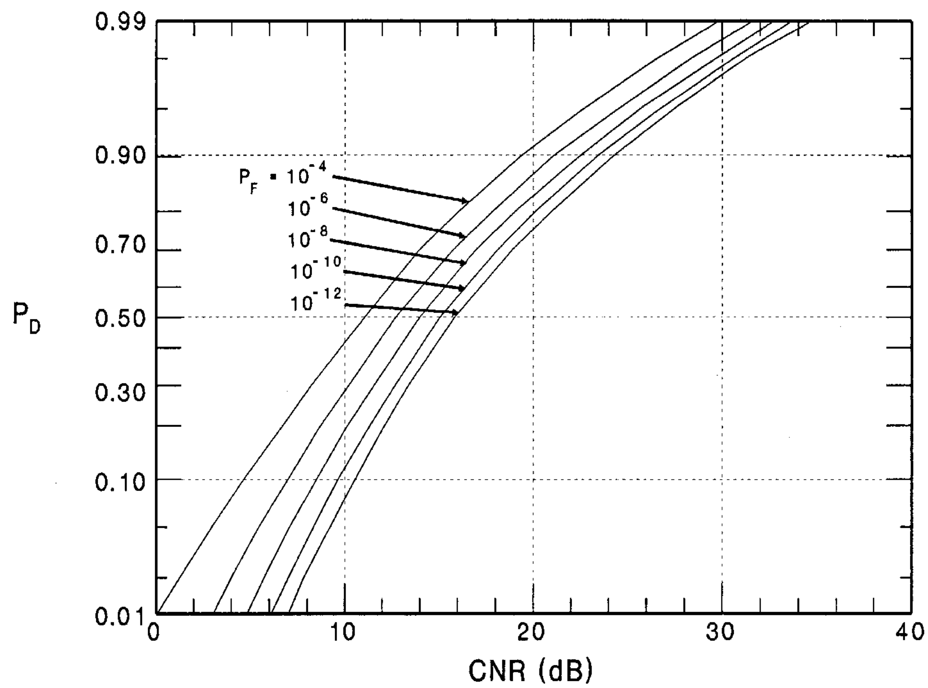


Figure E-6. Receiver operating characteristic for a Rayleigh fluctuating (Swerling 2) target.



For a cylinder of radius a and length L viewed at angle θ with respect to the cylinder broadside the cross section is

$$\sigma_{cylinder} = 4a\lambda\rho \cos\theta \sin^2(kL \sin\theta) / 2\pi \sin^2\theta$$

where λ is the radar wavelength and $k = 2\pi/\lambda$. For a cone of height H and cone half-angle θ_0 viewed nose-on the cross section is

$$\sigma_{cone} = (\lambda^2 \rho \tan^4\theta_0) / 16\pi .$$

When viewed at angle θ with respect to the nose the cross section is approximately

$$\sigma_{cone} = 2H \tan\theta_0 \lambda\rho \cos(\theta_0\text{-}\theta) \sin^2(kH \sec\theta_0 \tan(\theta_0\text{-}\theta)) / 2\pi \sin^2(\theta_0\text{-}\theta).$$

The broadside cross section is orders of magnitude larger (roughly $64\pi^2H^6/\lambda^3a^3$ larger) than the nose-on cross section. For a trihedral (or corner reflector or retroreflector – the bane of stealth design) with physical aperture A and viewed at angle θ with respect to the normal to the aperture, the cross section is given by

$$\sigma_{trihedral} = (4\pi A^2 \rho \cos^2\theta) / \lambda^2 .$$

Consider the Ballistic Missile Defense (BMD) radar example listed in the table. The radar cross section is representative of the cross section of a complete missile. The cross section of a separated reentry vehicle is expected to be much smaller (refer to the cross section expressions above). Note: cross sections of specific real missiles and reentry vehicles may differ by more than an order of magnitude larger or smaller than the representative values used here. However, since radar range scales as $\sigma^{1/4}$, an order of magnitude error in cross section yields only a factor of 1.78 error in range. This "BMD" radar will detect and track a ballistic missile at roughly 1000-km range. One face of this radar (4 are required for 360-degree coverage) has a power-aperture product of 1,770,000 W-m^2. One face is ABM treaty compliant. An aggregate of four faces might possibly be considered to be a single radar under the treaty. If it were, its power-aperture product would exceed treaty limits. Any attempt to push the detection range beyond 1000 km or to detect smaller cross section targets would likely cause even a single face to exceed the treaty limit.

Now let us consider the radar seeker example. These parameters are consistent with the active radar seeker of an anti-ship missile. Against a typical ship-sized target and given an uncluttered environment, this seeker will detect the ship at approx. 26 km (roughly equal to the radar horizon). There are several clutter and propagation effects present in the antiship missile problem that do not impact the BMD problem analyzed earlier. These include wave clutter, refractive ducting, and multipath.

The effective radar cross section of the ocean (or land) due to wave (or terrain) clutter is given by

$$\sigma_{clutter} = R \ \Delta\theta \ \Delta R \ \sigma_0$$

where $\Delta\theta$ is the angular resolution of the radar, ΔR is the range resolution of the radar, and σ_0 is the mean backscatter coefficient of the sea (or terrain). σ_0 is a function of radar frequency, observation angle (grazing angle), radar polarization, and sea state (or type and roughness of terrain). For Sea State 4 (the median encountered sea state in open oceans) and a radar frequency of 10 – 15 GHz the backscatter coefficient is roughly –29 dBsm/m2 at 10° grazing angle and roughly –48 dBsm/m2 at 0.1° grazing angle. At the maximum range of our hypothetical seeker and assuming a range resolution of 50 m and an angular resolution of 0.088 radians, we obtain a sea clutter cross section of only 1.8 m^2 at a typical sea-skimming angle of 0.1°. We also obtain a value of only 144 m^2 at an angle of 10° that corresponds to a typically pop-up-and-search-for-targets mode. Since ship cross sections are typically 10,000-m2 or even larger, sea clutter is not a serious problem.

Multipath interference can occur when the target and the ground (sea surface) are closer together than the angular resolution of the radar. Here it is possible for the radar radiation to take several different paths between the radar and the target and back. Some of the radiation may make an intermediate bounce off the ground before or after (or both) reflecting from the target. The signals from each of these paths will be temporally coherent but will have different phase shifts, resulting in interference between the signals. The instantaneous received power will fluctuate as the range or heights of the radar and target vary. For the simplest case (target, radar, and one reflecting surface), the power fluctuates as

$$P/P_0 \ \propto \ 16 \sin^4(k \, H_T \, H_R \, / \, R)$$

where P_0 is the power that would be received on the direct path alone, $k = 2\pi/\lambda$, H_T is the height of the target above the surface, and H_R is the height of the radar above the surface. This function goes to zero whenever

$$m = 2 \, H_T \, H_R \, / \, \lambda \, R$$

is an integer. As the range drops from infinity to zero, m will acquire integer values many times. When this occurs, detection of the target will be very difficult. In practice, for an antiship missile seeker, this is not really a problem. This "good luck" happens because a ship is a large target with radar scattering centers at a wide variety of heights. It is almost impossible that every scattering center could be in a multipath "null" at the same time. The numerous random interferences from multiple paths and multiple scattering centers contribute to the Swerling 2 (a model that assumes the target is composed of many small randomly phased scatterers) statistics assumed for the ship cross section.

Ducting occurs because there are irregularities in the strong gradients in water vapor density, temperature, and pressure in the atmosphere above the surface. These three factors influence the refractive index of the atmosphere at radar frequencies. In an ideal atmosphere, the refractive index decreases smoothly with altitude. However, when conditions are right, there may be a maximum of refractive index that occurs at an elevated height (typically a few meters to hundreds of meters). This is commonplace above water. Radiation emitted in the duct will tend to bend back towards this refractive index maximum. If the duct is strong enough and big enough, the radiation can oscillate back and forth many times about the index maximum. The duct effectively forms a waveguide. Radiation emitted outside the duct will tend to be bent in a fashion that moves it away from the index maximum at the fastest possible rate without oscillation. The implications on detection of low altitude targets by surface-based radars should be obvious. If both the radar and the target are in a duct, detection range may be vastly increased. If one is outside the duct and the other is inside the duct, then detection ranges will be drastically reduced because the radiation is directed away from the radar and/or the target. If the ducting structure can be determined ahead of time, there are computer codes that can indicate whether a specific cruise missile scenario will lead to increased or reduced detection range. For the missile seeker, regardless of whether the seeker is inside a duct or not, there will be parts of the target at heights that are inside the duct and parts of the target that are either above or below the duct. Ducting might help the detection performance of a missile seeker, but it will seldom hurt its detection performance. The same thing cannot be said about an air defense radar looking for low altitude cruise missiles.

Consider the third example in the table. Theoretically, the air defense/cruise missile defense (AD/CMD) radar is capable of detecting a cruise missile at the considerable range of 30 km. However, sea clutter, multipath, and ducting will seriously limit this performance. Consider first sea clutter. For Sea State 4, a grazing angle of 0.1°, and a frequency of 5 GHz, the backscatter coefficient is approximately –60 dBsm/m^2. Assuming a range resolution of 50 m and an angular resolution of 0.0132 radians, we calculate a sea clutter cross section of 0.02 m^2 at 30 km. This is equal to the 0.02 m^2 cross section of our assumed cruise missile (which was estimated based on a 20-inch diameter sphere with 10% reflectivity – a simplified model of the nose-on cross section of a Tomahawk). The radar will be as likely to detect a wave as it will a cruise missile. In fact because sea clutter will be present at all directions and in many range bins, waves will be detected far more often than the missile. As the missile gets closer, the sea clutter cross section will get smaller, and missile detection will become more probable.

Waves propagate at speeds of the order of ten m/s, while missiles move at hundreds of m/s. If the radar can measure target Doppler, then it is easy to eliminate sea clutter when searching for missiles. Unfortunately, many search radars do not have Doppler discrimination. The Doppler shift for a 100 m/s velocity at a frequency of 6 GHz is 4000 Hz. If the radar PRF is only 1000 Hz and it uses a complex quasi-cw waveform (such as FMCW or pulse Doppler) then it is theoretically capable of resolving a 25 m/s velocity. This would easily permit elimination of sea clutter. If, however, the pulsewidth or waveform duration is less than 80 μs, then the velocity resolution exceeds 300 m/s and Doppler discrimination is impossible.

Consider next the effects of multipath and ducting. Contrary to the missile vs. ship example, the ship vs. missile example has all of the missile scatterers located at what is effectively a single height. There is no averaging of multipath fades. As the missile closes on the ship, its signal strength will grow and fade with regularity, and the missile will appear and disappear from the radarscope. Assume the height of the radar is 30 meters and the altitude of the missile is 10 meters. The first multipath null occurs at 10-km range, the second at 5 km, the third at 3.33 km, etc. Since 10 km is roughly the range at which the target cross section appears to become dominant over sea clutter, the presence of multipath may significantly delay the detection. Ducting is also likely to occur. Because the missile and radar are at different altitudes, there is a possibility that the missile is in a duct while the radar is not, or vice versa. If this occurs, it can delay detection until extremely short ranges. The combination of adverse effects makes the problem of detecting and tracking cruise missiles at long ranges difficult. Unfortunately, if the missile cannot be detected at long ranges, it cannot be attacked at long ranges, negating much of the benefits of a layered defense.

APPENDIX F. THE 3X ACCELERATION HEURISTIC

In air defense missile design, a commonly-used heuristic or "rule or thumb" can be stated as "In order for an interceptor missile to reliably 'hit' a maneuvering target, the interceptor must be able to sustain turns with three times the acceleration that the target can sustain". Like any heuristic, this rule is only approximate, and is violated in a number of situations. However, the fact that a heuristic of this sort should exist can be determined in a straightforward manner. Consider two platforms moving directly towards each other and let one platform (the target) initiate a constant, maximum acceleration turn. The radius of that turn will be given by

$$r_T = v_T^2/a_T,$$

where v_T is the target velocity and a_T is the centripetal acceleration of the turn. Assume that the separation of the target and the second platform (the interceptor) is comparable to or less than the radius of the target turn, and that the interceptor begins its turn immediately after the target begins to turn. Then, for the interceptor to hit the target its turn radius must equal the target's turn radius. Any target that can outturn an interceptor can theoretically avoid being hit. Thus, using the equation above we must have the ratio of the centripetal accelerations equal to the inverse square of the ratio of velocities, that is,

$$v_I^2/v_T^2 = a_I/a_T.$$

Since interceptor velocities are usually higher (typically 1.5x to 3x) than target velocities (you want to be able to hit the target even if it is running away from you), the ratio of accelerations is invariably larger than one. If the interceptor is twice as fast as the target, its acceleration capability should be four times that of the target.

In real life, we must complicate the problem. First, if the target begins to turn too far away from the interceptor, then it turns out that the interceptor needs to pull only a mild turn to correct its trajectory. This is true, because at sufficiently long range, the angle subtended by the target's turning circle can be arbitrarily small. It is unlikely that a piloted aircraft will initiate its turn at the perfect separation to require the interceptor to pull the maximum acceleration. Second, the engagement geometry is seldom head-on. In a complex geometry, there is a turn direction that maximizes required interceptor acceleration. All other directions require less than maximum acceleration. A piloted aircraft may choose a less than optimal turn direction (regardless of pilot skill, although training will reduce avoidable errors). There are unavoidable errors, as it is possible that the optimum turn direction would cause the target to experience even greater hazards, such as flying into the ground. Third, most missiles have proximity fuzes. They only need to get close to the target not hit it. This leads some ballistic missile defense "wags" to comment that that is why missiles are called "miss"iles not "hit"tiles (BMD kill vehicles are occasionally referred to as hittiles). Fourth, the interceptor cannot detect the turn immediately; it must wait until the actual target motion deviates significantly from its predicted motion. This time delay to initiation requires larger accelerations to match the target's turn. The first three complications reduce the required interceptor acceleration; the fourth increases it. Taking all factors together, and considering an average over all combinations of interceptors, targets, and geometries, the missile industry has arrived at its 3-to-1 acceleration heuristic. Obviously, the heuristic will break down if there is a very large velocity differential between target and interceptor. It may also break down whenever manned targets are replaced by “intelligent”, unmanned targets.

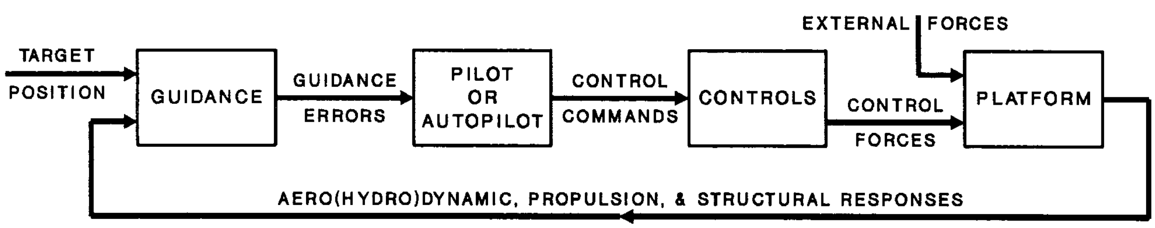
APPENDIX G. PRINCIPLES OF MISSILE GUIDANCE

INTRODUCTION

Missiles may be guided to their targets by many different approaches. Many of these approaches are listed in Table G-1, although the list is far from complete. In the following we will describe these guidance techniques in more detail. However, regardless of the technique used, certain principles apply to all guidance problems. Although the term missile will be used throughout, it should be noted that the navigation and guidance techniques described here can apply to any platform, whether manned, remotely controlled, or autonomous, and whether underwater, surface-bound, airborne, or exoatmospheric. Indeed, some of the guidance approaches find limited applications in missiles, and far more application in other platforms.

Figure G-1 describes in some detail a generic guidance and control model. Whether the missile is guided by an active seeker, a semi-active seeker, a passive seeker, command guidance, or beamrider, or whether the guidance employs radio frequency or infrared radiation, the guidance problem can be described at the top level by this model. Although we will emphasize the guidance subsystem of this model, the characteristics of the complete feedback loop are sufficiently important to warrant special mention.

Figure G-1. A generic guidance and control model.



The guidance subsystem contains the sensor (seeker), inertial reference, and processor necessary to compare actual missile motion to the desired missile motion and derive guidance errors. The autopilot (or pilot in a manned system) converts guidance errors into commands suitable for actuating the motion control system. Frequently, complex transformations and nonlinear gains must be applied to the guidance errors in order to accomplish this. In a manned system the pilot may fulfill both the guidance and autopilot functions without augmentation from other hardware. The motion controls act upon receipt of control commands to apply forces to the missile in order to alter its motion. The applied forces may be aerodynamic/hydrodynamic (produced by canards, fins, ailerons, elevators, rudders, or the body of the missile), frictional (produced by wheels, tracks, or runners), or propulsive (produced by tilting rocket nozzles, exhaust vanes, divert motors, etc.). In addition to control forces, the missile is subject to external forces, such as gravity, buoyancy, winds, ocean currents, blast forces, and turbulence, as well as drag and thrust (propulsion). The forces applied to the missile will elicit changes in center of gravity motion and orientation. In addition, static and dynamic structural deformations will occur. These

Table G-1. Types of missile guidance.

NAVIGATION	* CELESTIAL	- STAR TRACKERS	
	* INERTIAL	- STRAPDOWN INERTIAL MEASUREMENT UNIT - STABLE TABLE INERTIAL PLATFORM	
	* DOPPLER		
	* CORRELATION ("MAP" READING)	- TERRAIN CONTOUR MATCHING (TERCOM) - SCENE MATCHING	
	* RADIONAVIGATION	- HYPERBOLIC (e.g., LORAN) - RANGE-BASED (e.g., GPS) - DIFFERENTIAL (e.g., DIFFERENTIAL GPS)	
RADIO-FREQUENCY	* ACTIVE RADAR	- CON-SCAN RADAR - MONOPULSE RADAR - TRACK-WHILE-SCAN RADAR	
	* SEMI-ACTIVE RF		
	* COMMAND		
	* ANTI-RADIATION HOMING		
	* BEAMRIDER	- CON-SCAN RF BEAM - MULTIPLE-BEAM	
INFRARED	* PASSIVE NON-IMAGING	- RETICLE	-- SPIN-SCAN vs CON-SCAN -- AM vs FM -- ONE-COLOR vs TWO-COLOR
		- CON-SCAN CROSS DETECTOR ARRAY	
	* PASSIVE QUASI-IMAGING	- ROSETTE SCAN - SPINNING LINEAR ARRAY	
	* PASSIVE IMAGING	- SCANNED LINEAR ARRAY - MULTI-COLOR SCANNED LINEAR ARRAY - STARING FOCAL PLANE ARRAY - MULTI-COLOR STARING FOCAL PLANE ARRAY	
	* SEMI-ACTIVE LASER (DESIGNATOR)	- QUAD-CELL LASER SPOT TRACKER - IMAGING LASER SPOT TRACKER	
	* BEAMRIDER	- TEMPORALLY-ENCODED LASER BEAM - SPATIALLY-ENCODED LASER BEAM	
	* COMMAND	- RF COMMUNICATION LINK - WIRE COMMUNICATION LINK - LASER COMMUNICATION LINK - FIBER-OPTIC COMMUNICATION LINK	
	* ACTIVE	- SCANNING LASER TRACKER - IMAGING LADAR	

deformations interact with the motional changes. Consequently, the motional changes do not occur instantly, nor are they exactly the desired changes.

The guidance subsystem employs a model for the desired motion in order to determine the error signal to be generated for any given seeker measurement. These models are commonly called guidance laws. The simplest law is **straight-line** guidance. Any measurement that differs from that which would be generated if the missile moved in a straight line, produces an error signal proportional to that difference. This type of guidance law is employed in very short range missiles (e.g., a light antitank weapon) targeted against slowly moving or stationary targets. **Line of sight** guidance is another common guidance law. The missile is assumed to be following a straight line along the line of sight from a sensor. Any deviations detected from this predicted motion will produce an error signal. Note that this law differs from straight-line guidance in that the straight line used to define proper motion can vary in time. The line of sight does not need to be stationary. Line of sight guidance is commonly used in command-guided or beam-rider-guided missiles. **Offset line of sight** guidance is the same as line of sight guidance except that the expected line of missile motion is offset from the true line of sight by a constant angle. It is used when it is desired that the missile should miss the target by a short distance. One application is in top-attack anti-tank weapons. The missile is aimed to pass just above the turret of a tank. As it passes the fuze fires a side-directed shaped charge down onto the turret. This is offset line of sight guidance because the gunner tracks the tank not the empty space above the tank. A fourth guidance law is **pursuit**. The expected motion is assumed to follow a straight line from the seeker to the detected target. It is called pursuit guidance because the missile chases the apparent target position and in many cases will wind up attacking the target from the rear quarter. It is seldom used. A more commonly used law is **proportional** guidance or proportional navigation. The missile is assumed to follow a path that is a straight line between the seeker position and the predicted position of the target at the predicted time of impact. In practice, this path is the path that provides zero line of sight rate of the target in the seeker field of view. If the target has a line of sight motion relative to the seeker, an error signal is generate. This guidance law is used by almost every homing seeker.

Missile guidance and control loops can be characterized by a missile time constant. This is the time required for an error to be translated into control commands, the commands to be applied to the controls, and the resulting airframe responses to interact with each other and stabilize. A valuable heuristic in aircraft interceptor missiles is that the time constant is usually in the range 0.1-0.2 seconds. This range of time constants is consistent with being able to follow the maneuvers of a nominal target capable of performing 10g maneuvers, without overdesigning the agility of the missile. After a target maneuver occurs, it takes time for the missile to make a compensating maneuver and to stabilize its flight on the new trajectory. Typically, the time required for this to occur is 10-20 missile time constants (1-4 seconds for an interceptor missile). Each measurement of guidance error (difference between the measured target position and the estimated position which the missile has been using to determine control commands) will itself be somewhat in error due to sensor noise, random motional disturbances, etc. Rather than have the missile respond to this noise, the guidance error measurements are filtered (e.g., with a Kalman filter). This results in 5-10 guidance error measurements being required per missile time constant.

These fundamental design concerns lead to several obvious consequences. First, guidance measurement intervals in interceptor missiles are typically between 0.01 and 0.04 seconds (corresponding to 25-100Hz rates). Secondly, terminal phase guidance must begin at least 1 to 4 seconds before predicted impact, or the missile will be unable to make any desired trajectory corrections and stabilize its flight path. The exact values required depend on the missile time constant and the integration time of the guidance filter. The most important consequence is that once the missile designer has selected a guidance technique, many of the parameters he might wish to vary are fixed within narrow limits by the fundamental requirements imposed by the need for achieving good guidance.

NAVIGATIONAL GUIDANCE

Navigational guidance attempts to move the missile (or any other guided platform) from one position in space (presumably known with accuracy) to another position in space (also presumably known with accuracy). There are at least five classes of navigational guidance: celestial, inertial, Doppler, correlation, and radionavigation. They are commonly employed when transit times and/or distances are long.

Celestial navigation uses star trackers to search at least three selected star fields, analyze the patterns, identify pre-cataloged reference stars, and determine (from the stellar lines of sight) the orientation of the missile relative to the "fixed stars". Coupling this information with the direction of the center of the earth (usually determined from the direction of the gravitational force, although it could be determined by other means) confines the missile location to lie on a specific half-line that extends outward from the earth's center. Knowledge of the precise time (from a stable clock) permits the rotation of the earth to be taken into account and allows the intersection of the half-line with the earth's surface to be uniquely determined. Altitude above the surface of the earth, if it is required, must be determined by other means. These might include radar, determination of the magnitude of the earth's gravitational attraction (the force falls off as $1/r^2$ where r is the missile distance from the earth's center), or angular extent of the earth's disk.

Inertial navigation uses an inertial measurement unit (IMU) consisting of three accelerometers oriented along orthogonal axes and three gyroscopes whose "input" axes coincides with the axes of the accelerometers. Each accelerometer measures the component of missile linear acceleration lying along its measurement axis and each gyro measures the component of missile rotation rate along its input axis. Use of this information depends on how the IMU is oriented with respect to the missile. In a stable table inertial platform, the IMU uses its gyroscopic characteristics to maintain a constant precise alignment to a fixed external coordinate system called the inertial reference frame. No matter how the missile moves, the stable table always remains aligned to the inertial frame. Continuous acceleration measurements along each axis can be doubly integrated with respect to time to yield the change in position along that axis.

$$r_i(t) = \int_0^t dt \int_0^t dt \, a_i(t) \qquad \text{where } I = x, y, \text{ or } z$$

At any point in time, simple measurement of the orientation of the stable table with respect to the missile yields the orientation of the missile with respect to the inertial reference frame. In a strapdown inertial system, the axes of the IMU are permanently aligned to the missile. Continuous rate measurements from each gyro may be singly integrated over time to give the angular position of the missile about each axis relative to the initial angular position. The angular data is used to transform the instantaneous accelerometer data (measured in missile coordinates) into accelerations measured with respect to the inertial frame. Doubly integrating the continuously transformed accelerations over time gives the actual position of the missile in inertial coordinates relative to its initial position.

Doppler navigation systems use radars transmitting in three non-collinear directions. The Doppler shift of the radar return along each direction is measured, corrected for missile rotation rate (which will induce additional, but predictable, Doppler shifts) using gyroscope data, and used to determine the vector direction and magnitude of the missile velocity. Singly integrating the velocity over time gives the missile position relative to its initial position.

Correlation navigation involves using sensors to measure some characteristic of the external environment at a preselected waypoint and correlating the measured characteristic against reference characteristics previously measured and stored as a function of spatial position. This is the electronic equivalent of a traveler reading street signs and using the observed street names to find his location on a map. One implementation of correlation guidance is terrain contour matching (TERCOM). A radar altimeter measures the altitude of the missile over an extended path. Assuming the missile moved in a straight line, the collected altitude measurements can be readily converted to a terrain elevation profile. If the motion is not straight line, then an IMU can provide needed corrections. The terrain profile is correlated both in angle and position against a stored terrain map. The highest correlation will be obtained when the measured profile precisely overlays a stored map profile. The position and orientation (direction of motion) can be determined directly. Scene matching uses an imaging sensor to acquire an image of a portion of the outside scene. After appropriate image processing, the acquired scene can be correlated against stored reference scenes. The location associated with the stored scene that gives the best correlation against the measured scene gives the missile position. With a few dozen (or less) waypoints and given moderate accuracy inertial guidance in between, a missile can be navigated with fractional kilometer accuracy over many thousands of miles.

Radionavigation systems employ radio frequency emissions from multiple transmitters. Based on the signals detected by a receiver, the position can be calculated. One class of radionavigation systems is **hyperbolic** in nature. The transmitted signals are used to detect the difference between the distance between the receiver and one transmitter and the distance between the receiver and a second transmitter. The curve of possible positions for a specific measured distance difference is a hyperbola. If the distance difference between the receiver, one of the first two transmitters, and a third transmitter is also measured, a second hyperbolic solution is generated. The intersection of the two hyperbolas establishes the receiver position. LORAN is a common example of a hyperbolic system. LORAN chains consists of a master station and several slave stations located roughly 1000 miles apart. All stations transmit pulsed signals at a carrier frequency of 100 kHz. The master station transmits its signal first, and as soon as each slave station receives this signal, it transmits its own signal. The process is repeated roughly every 0.8

to 1.0 seconds. The repetition interval is unique and is used to identify the specific chain being detected. The time difference between reception of the master signal and a slave signal is the distance difference divided by the speed of light (minus a small known correction for retransmission delay in the slave stations). Reception of the master and two slave signals permit identification of receiver position (with the possibility of the mirror image uncertainty). Reception of the master and three slave signals permits unique identification of the receiver position.

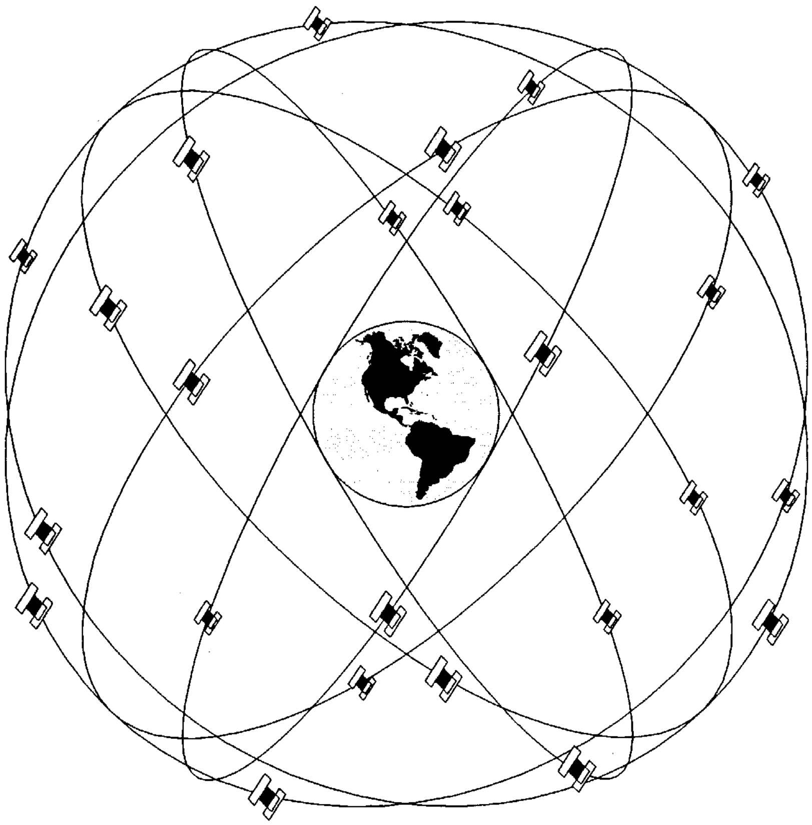
Range-based radionavigation systems invariably involve satellite transmitters and use a large constellation of satellites. The constellation is designed to place at least 4 satellites above the horizon at any selected time and at any geographic position. The satellites transmit timing signals. From these signals, the line of sight distance to each satellite can be calculated. Knowledge of one distance limits position to lie on a sphere. Addition of a second distance permits isolation to a circle (the intersection of two spheres is a circle). Addition of the third distance permits isolation to one of two points (the intersection of a sphere with a circle is two points). Addition of a fourth distance permits selection of the proper point. However, one of the two points usually lies at an unreasonable position or is moving at an unrealistic velocity. For example, in GPS one point usually lies within the sphere of satellite orbits, while the other lies outside. Usually, it is easy to tell whether you are near the surface of the earth or in deep space. Thus, only three distance measurements would seemingly suffice. Usually, however, there are other reasons to require four measurements.

In the **Global Positioning System (GPS)** the satellite constellation involves at least 24 satellites placed in six orbital planes – spaced 60° apart, inclined at an angle of 55° with respect to the equator, and containing four satellites apiece (roughly illustrated in Figure G-2). Each satellite orbits at a distance of roughly 20,200 km with a period slightly less than 24 hours. In reality there are usually more than 24 satellites as replacements are launched in advance for those satellites nearing the end of their operational lifetimes. This constellation guarantees that five to eight satellites are above the horizon at any time and at any point on the surface of the earth. Each satellite carries an atomic clock to provide for the transmission of its coded signals in perfect synchronization with every other satellite.

The satellite signals are basically pseudo-random noise (PRN) binary codes. The distance from a satellite is determined by correlating the code received from the satellite against the code generated by the receiver. The time displacement of the peak of the correlation function is the time required for the signal to propagate from the satellite to the receiver. By multiplying by the speed of light the distance to the satellite can be calculated. The position of the satellite is encoded into the satellite's message. The receiver can decode this message, and use the orbital parameters (ephemeris data) transmitted to calculate the satellite's position at any point in time. When coupled with the calculated distance this permits the calculation of the position sphere for that measurement. Three such measurements theoretically permit determination of position.

However, there is a problem. The satellites carry expensive atomic clocks to permit synchronization. The receivers cannot afford to carry expensive clocks. The use of inexpensive

Figure G-2. A rough illustration of the GPS satellite constellation.



clocks means that the time used by the receiver to generate the start of its code sequence will differ by a small amount from time used by the satellites to generate the start of their code sequences. This time error translates directly into position errors. For example, a tiny error of only 1 microsecond translates into an unacceptable 300-m distance error. This problem is why four satellite measurements are required. The time error is the same for the signal from every satellite (the receiver's clock is the one with the error). If four measurements are compared using this same error, then at most three of the distances can be made to intersect at a point. The fourth will not match. However, if a constant error is subtracted from each distance, the intersection characteristics will change. When the true constant error is subtracted from each distance, all four measurements will intersect at a single point. By trying a number of possible constant errors until a four-measurement intersection, the timing error can be effectively eliminated and an accurate position determination can be achieved.

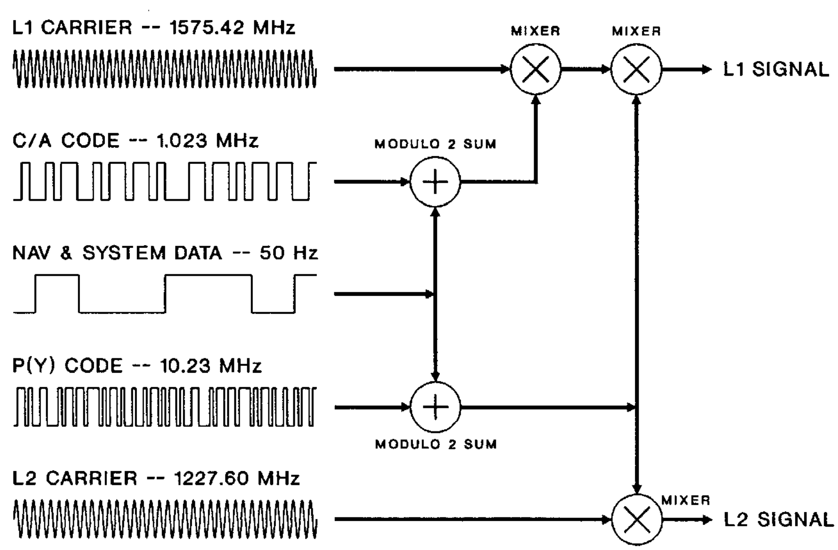
There are a number of other factors that influence accuracy. One of these is the refractive index of the ionosphere, which changes as a function of time. The refractive index reduces the speed of light. If the actual speed of light (due to the ionosphere) is less than the value assumed in the calculation, then the distance estimated from the time delay will be larger than the actual value. GPS actually transmits two coded signals at carrier frequencies L1 (1575.42 MHz) and

L2 (1227.60 MHz). The ionosphere delays each one differently. By measuring the difference in delays, the ionospheric delay can be eliminated.

The L1 carrier phase is modulated by a PRN code called the clear/acquisition (C/A) code. This code has a bit time of roughly 1 μs and repeats every 1023 bits (one millisecond). This code spreads the spectrum of the L1 carrier over a 1.023 MHz bandwidth. Each satellite has a different C/A code. The C/A code is the basis of the Standard Positioning Service (SPS) which is available to all users, civilian or military. Civilian receivers only need to receive the L1 carrier and are provided with the PRN codes of every satellite). The SPS guarantees accuracy (two standard deviations) of at least 100 meters horizontal accuracy, 156 meters elevation accuracy, and 340 nanoseconds time accuracy, under standard conditions. Under a program of selective availability (SA), the Department of Defense intentionally degrades the accuracy of the C/A code by using a time-varying bias (the actual time of transmission is dithered around the atomic clock-specified time of transmission by a small amount that varies over hours-long time scales. Each satellite has a different random bias applied. The errors induced by the biases preclude any measurement using the C/A code from having a guaranteed accuracy better than the SPS standard.

The carrier phases of both L1 and L2 are modulated by a second PRN code called the precise (P) code. This code is modulated at 10.23 MHz rate and has a repeat length of a week. The P code is further encrypted into the Y code. The complex code followed by encryption makes spoofing (generation of false P coded signals) almost impossible. Authorized (military) users can obtain receivers that contain decryption electronics permitting the P code to be used for timing. Timing derived by correlation of the P codes is the basis for the Precise Positioning Service (PPS). The PPS guarantees accuracy (two standard deviations) of at least 22 meters horizontal accuracy, 27.7 meters vertical accuracy, and 100 nanoseconds time accuracy, under standard conditions. The generation of the L1 and L2 signals from the individual data streams is summarized in Figure G-3.

Figure G-3. Generation of the L1 and L2 signals.



The use of PRN codes in GPS serves several purposes. First, it permits the extraction of the timing information. Second, the spread spectrum nature of the code adds an inherent jam resistance. Noise introduced by jamming at a single frequency is effectively reduced by the ratio of the jammer bandwidth to the spread spectrum bandwidth. However, the anti-jamming margin provided by spread spectrum techniques does not preclude jamming. Spread spectrum only makes jamming more difficult. PRN codes also permit "processing gain" to be achieved through integration over extended periods of time. This gain is essentially the spread spectrum bandwidth over the integration time. The high processor gains permit very small receiver antennas to collect enough signal intensity to produce an acceptable signal-to-noise ratio after the antenna gain is included.

For some applications even the accuracy available from PPS is inadequate. **Differential** measurements can frequently overcome those limitations. Consider placing a receiver at a position whose position is accurately known from traditional surveying methods. The position measured by the GPS system can be compared to the known position and the "correction" can be transmitted to other receivers in the area. The correction is due entirely to errors caused by the nature of the GPS system. However, any receiver located within a limited distance of the "reference" receiver will have almost exactly the same GPS-produced errors at the same time as the reference receiver. Therefore the correction derived from the reference receiver can be applied to the measured value from the second receiver. The corrected value will now have accuracy comparable to the residual errors (due to the initial surveying) of the reference location.

If a reference location is unavailable, a different differential approach might still be valuable. For example, two receivers at unsurveyed locations can make GPS measurements and compare them. Since each receiver will have roughly the same GPS-produced error, the difference between the two measurements will be an accurate measurement of the relative distance between the two receivers. Coupled with accurate angle measurements from passive targeting sensors, accurate knowledge of the baseline can permit accurate passive ranging to the target.

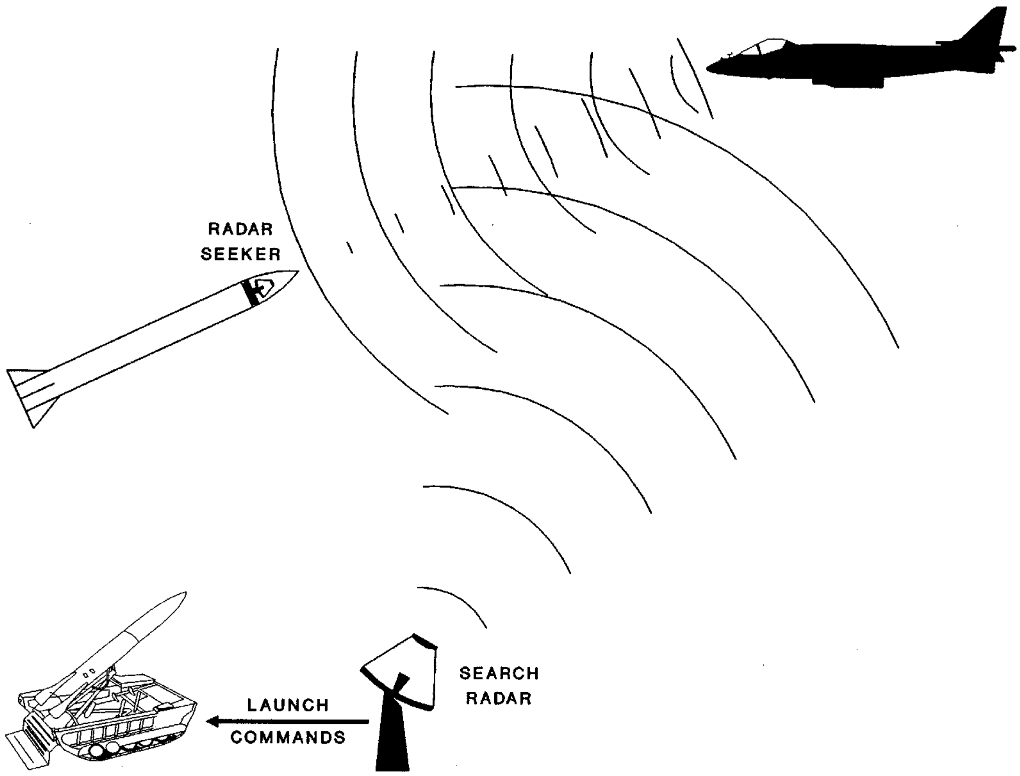
RADIO-FREQUENCY GUIDANCE

Radio-frequency guidance employs sensor systems operating in the radio frequency or microwave regions of the electromagnetic spectrum to determine the information needed for guidance. There are five major classes of radio-frequency guidance: active radar, semi-active radar, command, anti-radiation homing, and beamrider.

Active Radar

Active radar guidance employs seekers containing microwave radar sensors. Refer to Appendix E for a technical discussion of radar. Figure G-4 illustrates active radar guidance. After initial flyout in the direction of the target (most likely using inertial guidance and initial target positions derived from a search radar), the seeker radar transmits electromagnetic radiation in the general direction of the target. The target reflects a small fraction of the radiation that is subsequently detected by the seeker radar. The angle of arrival of the radar return relative to the missile axes is used to derive a guidance error signal.

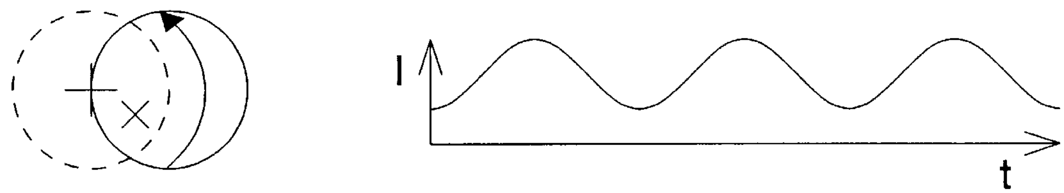
Figure G-4. Active radar missile guidance.



Radar seekers are likely to employ one of three tracking modes: track-while-scan, conical scan (con-scan), or monopulse. Track while scan systems sweep out a large field of view with a relatively narrow beam. Every threshold crossing in the received signal is recorded on a scan cycle. These are correlated against threshold crossings on subsequent scans. Likely targets are assigned to track files, data from each file being processed by a track filter. One target is designated by the system or the operator (based on any of a number of criteria). The location of the designated target relative to the nominal center of the field of view is used to determine the guidance error.

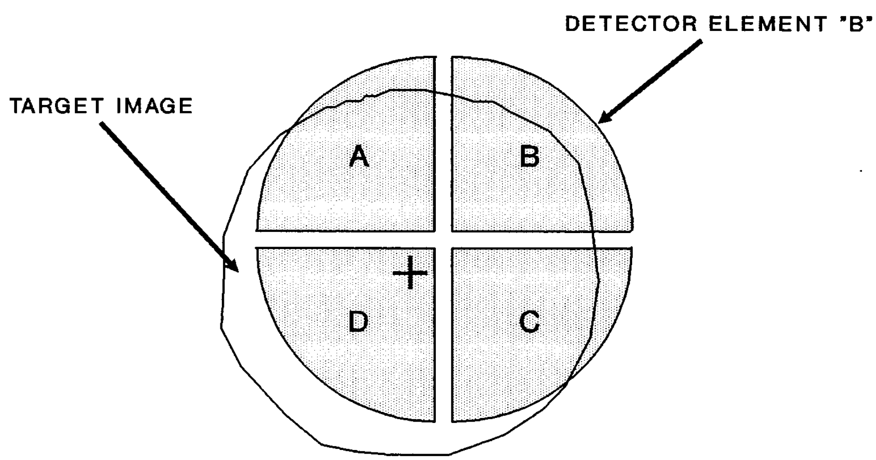
Conical scan systems use a moderate width radar beam that is circularly swept about a fixed direction, as shown in Figure G-5. This results in the beam sweeping out a conical region of space. If a target is located at the center of the circle defining the conical scan (the + in the figure), then the edge of the beam continually illuminates the target and the radar return will be constant (except for cross section fluctuations). If the beam is not at the center of the conical scan (e.g., at the **x** in the figure) then part of the time the target will be near the center of the radar beam and part of the time the target will be distant from the center of the radar beam. The intensity of the radar return will be amplitude modulated at the scan frequency. The magnitude of the amplitude modulation is linearly proportional to the radial distance of the target from the center of the conical scan.

Figure G-5. Conical scanning and tracking.



Monopulse radar systems transmit broad radar beams and have four closely spaced receivers (see Figure G-6). If a target is located exactly at the center of the radar beam, then each receiver will see a return of exactly the same amplitude and phase. If the target is located an angular distance away from the center of the beam, then amplitudes on some of the receivers will be larger than the amplitudes on other receivers. The phases of the signal will also differ from receiver to receiver. In a monopulse system, the phases (or amplitudes) of the four receiver outputs are summed and differenced in such a way that horizontal and vertical error signals are produced (as shown in the Figure). These signals are linearly proportional to the target's angular distance away from the beam center.

Figure G-6. Error signal generation in a quadrant detector (or a monopulse radar).
A, B, C, D in the equations represents the signal strength being generated
by detector quadrant A, B, C, D, respectively.



HORIZONTAL ERROR

EH = ((A+D)-(B+C))/(A+B+C+D)

VERTICAL ERROR

EV = ((A+B)-(D+C))/(A+B+C+D)

Active radar seekers are susceptible to the same kinds of countermeasures as are all radars of comparable design. For example, con-scan seekers with doppler discrimination are susceptible to inverse gain jamming or velocity gate walk-off just like their equivalent surface-based analogs. Chaff may provide an attractive decoy to active seekers.

Semi-Active Radar

Semi-active radar guidance employs seekers containing microwave receivers, as illustrated in Figure G-7. An external sensor such a radar is used to detect and track the target. This tracking information is used to point a microwave illuminator beam at the target. The target reflects some of this radiation, which is subsequently detected by the receiver in the seeker. The angle of arrival of the reflected signal relative to the missile axes is used to derive a guidance error signal. Conical scan and "monopulse" receivers are two techniques commonly employed to obtain the angular information about the target position relative to the missile location.

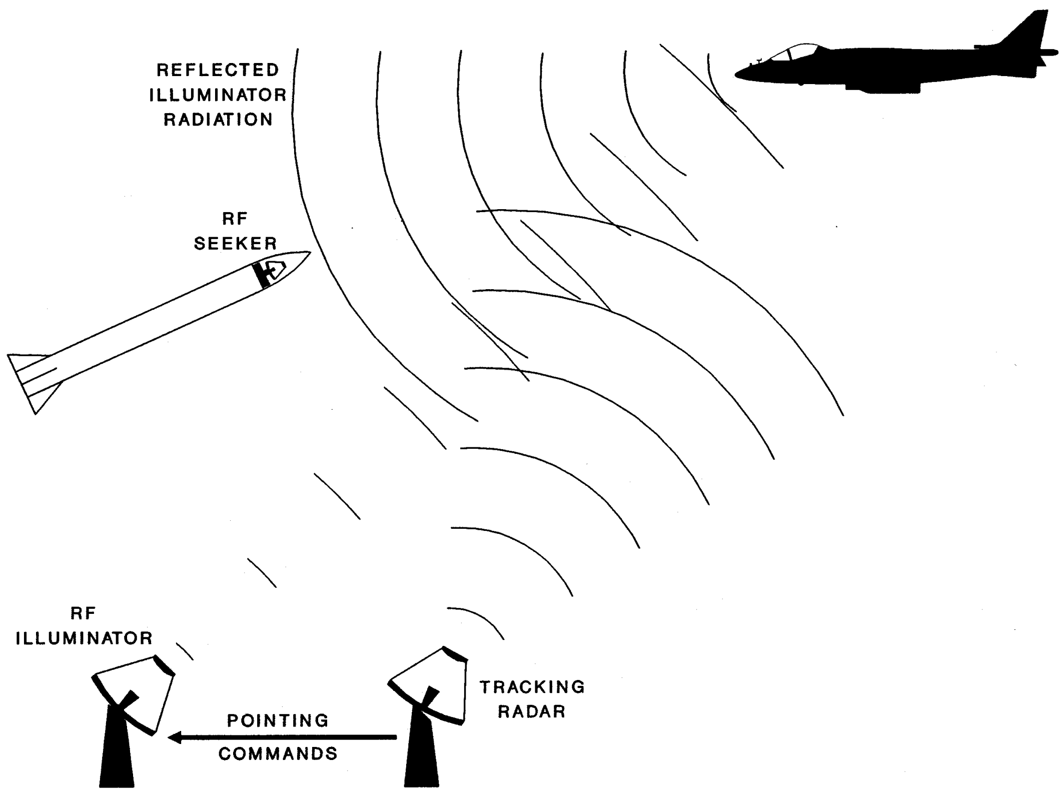
Semi-active guidance implements a form of bistatic radar. Bistatic radars have transmitters and receivers located at different locations. The detection performance of a bistatic radar is given by a "radar equation" in which

$$CNR = P_{AV}\, \pi D_T^2\, D_R^2\, \sigma\, exp[-\alpha(R_R + R_T) / 64\, k\, T\, PRF\, F\, \lambda^2\, R_R^2\, R_T^2$$

This is the same as the radar equation derived in Appendix E, except that the fourth power of the radar transmit/receive aperture is replaced by the product of the squares of the transmit (illuminator) aperture and the receive (seeker) aperture, and the range has been replaced where appropriate by the range between the illuminator and the target R_T and the range between the target and the seeker R_R. The bistatic radar cross section may differ from the cross section for a traditional radar. For conventional targets, the average difference in cross section will be small; for stealth targets, it is possible that the bistatic cross section is much larger than the traditional radar cross section. The anticipated receiver operating characteristics should be essentially the same.

Semi-active radar missiles are not immune to countermeasures. Chaff may provide a strong decoy reflection that will seduce the missile seeker away from the target reflection. The geometry provides for main lobe coupling of self-defense jammer radiation into the seeker. Noise jamming may be effective against all kinds of semi-active seeker. A strong sinusoidal AM at frequencies near the scan frequency of a conical-scan seeker may also prove effective. However, the nominal $1/R_R^2$ dependence of the semi-active seeker performance tends to make it less sensitive to jamming signals than active radar seekers with their $1/R^4$ dependence.

Figure G-7. Semiactive radar missile guidance.

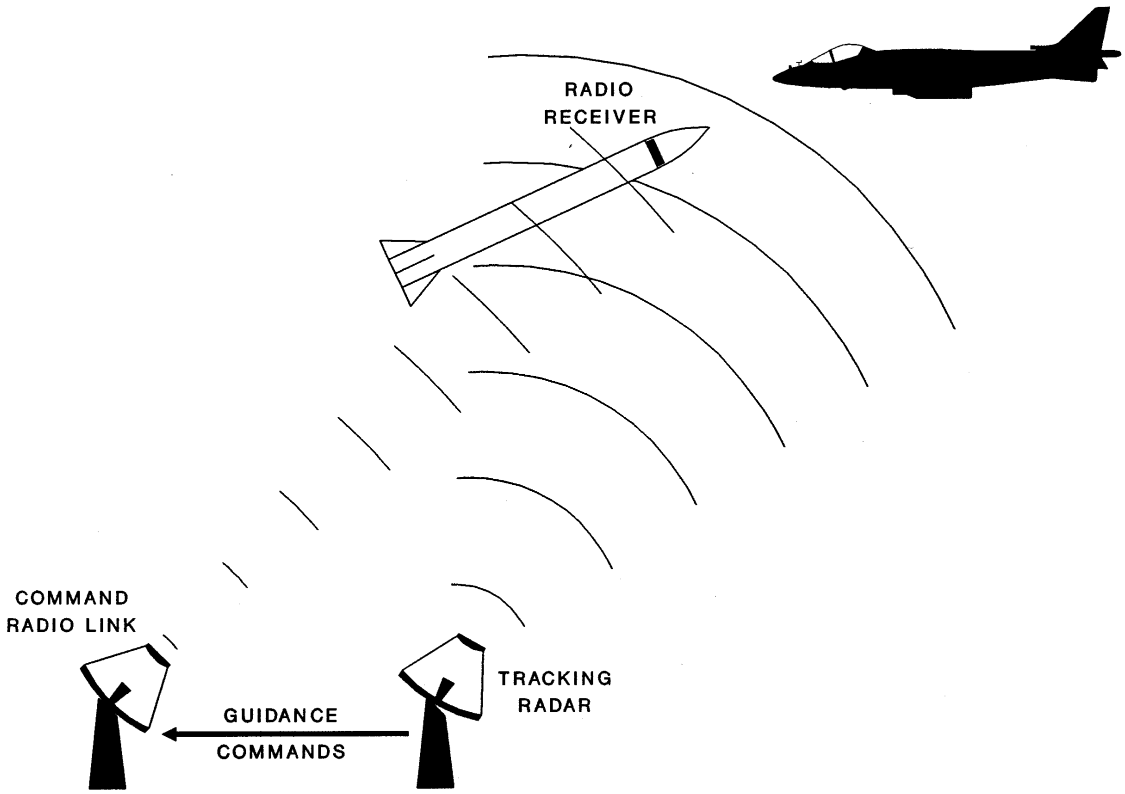


Command

In a command guidance system, a fire control radar (occasionally an electro-optical sensor such as a television may augment the radar) detects and tracks the target and also tracks the missile. A processor in the fire control system computes the guidance errors and transmits specific guidance commands (up/down, left/right, and how much of either) to the missile. The missile receives these commands and adjusts its control surfaces accordingly. The commands from the fire control system are commonly transmitted to the missile via a radio frequency communication link.

Command guidance of missiles can be countermeasured in two distinctly different ways. In the first technique the guidance link between the fire control and the missile may be jammed. Unfortunately, the range of communication frequency options (HF to millimeter-wave) may exceed the spectrum coverage of the jammers. The second alternative is to jam the tracking radar of the fire control system. If electro-optical adjuncts to tracking are available, then fire control radar jamming will be ineffective.

Figure G-8. Command missile guidance.

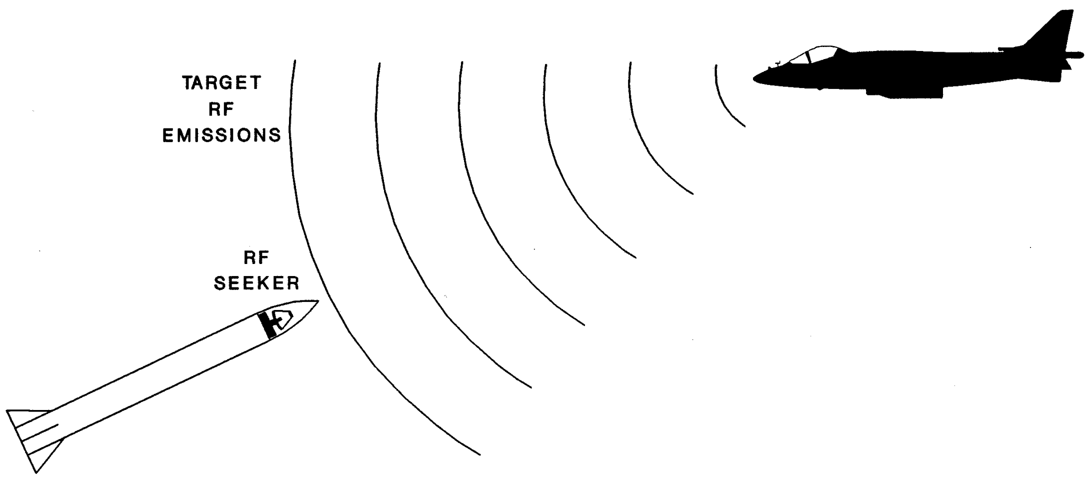


Anti-radiation Homing

Anti-radiation homing guidance (shown in Figure G-9) employs a seeker containing directional microwave receivers. If the target emits microwave radiation, the receiver in the seeker will detect it and determine its angle of arrival. This is subsequently used to derive a guidance error signal. Common receivers used for anti-radiation homing are “monopulse” and conical scan. Anti-radiation missile homing is seldom used against aircraft. Its more common application is to attack and destroy enemy air defense radars on the ground. The Suppression of Enemy Air Defenses (SEAD) mission relies heavily on anti-radiation homing missiles. However, anti-radiation homing missiles may find a significant application in attacking high-value airborne radar assets such as AWACS or J-STARS.

Anti-radiation homing guidance is difficult to jam or decoy. The most common tactic is to turn the radar off and on intermittently, thus denying continuous signals to the seeker. This may be done independently or in concert with other nearby radars. A second radar may come on-line to take over the job of the first radar which is shutting down. Blinking between radars may confuse some anti-radiation homing missiles. It may attempt to acquire each new target as it becomes strongest and will ultimately impact somewhere in between the blinking radars. However, once a more modern anti-radiation homing missile has acquired a lock on an emitter, it may be difficult for that emitter to avoid destruction. It is possible for the missile to inertial

Figure G-9. Anti-radiation missile homing.



guide itself in the direction of the last good radar emission. Although accuracy will not be as high as if the radar had been kept on, anti-radiation missiles usually have warheads with large kill radii (100 meters) against soft targets such as radar vans and antennas. If the radar waits too long before turning off, the inertial follow-up accuracy will likely be high enough to produce a kill. The seeker may have an infrared imaging adjunct that acquires a separate track on the suspected emitter. The infrared image will not disappear if the rf emissions disappear. The infrared guidance accuracy may even exceed the anti-radiation homing guidance accuracy. Lastly, if a cruise missile is equipped with an anti-radiation homing seeker, the missile may be able to loiter over a suspected radar site until the radar turns on again. Each time the radar blinks on, the loitering missile refines its estimate of the target location, until the missile is certain enough of the location to attack and destroy it. Thus, shutting down the radar will not prevent its destruction. Even if the radar can survive by shutting down, any radar that is not radiating is a radar that is not a threat.

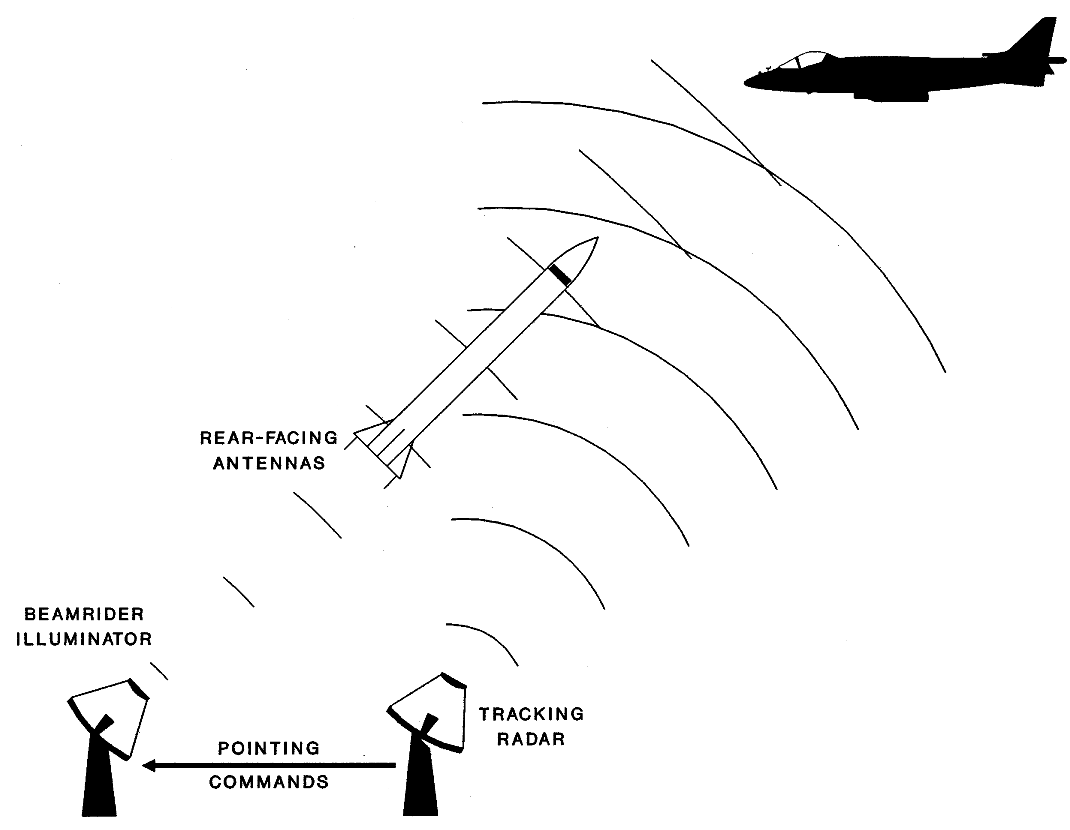
Beamrider

In a beamrider a beam of microwave radiation is projected along the path that the missile should follow. Refer to Figure G-10. The pointing information is typically generated by a separate tracking radar used for fire control. The beamrider beam has spatial characteristics that are detected by receivers on the aft end of the missile. These characteristics are used by the missile to determine where it is located with respect to the center of the beam. Corrections to the missile motion are used to bring it to the center of the beam and keep it there. The missile will then ride the beam until it intercepts the target (assuming of course that the beam intercepts the target).

There are a variety of concepts for using a beamrider to give spatial information to the missile. In some beamrider systems a simple conical-scanned beam is employed. If the missile is not at the center of the conical scan, the aft receivers will detect an amplitude-modulated signal at the scan frequency. Once the missile is centered on the scan, the amplitude modulation will disappear. The magnitude of this modulation is linearly related to the angular displacement from the center of the conical scan. In another beamrider implementation, four beams are transmitted along directions separated by a beam width. Each beam carries a different modulation. The aft receivers on the missile detect the modulations. The relative amplitude of each signal is used to determine the direction and distance of the missile from the center of the multiple beams. When the signal strengths of all four beams are equal, the missile is at the center. One version of this has the "up" beam transmit a series of long pulses with short spaces between pulses. The "down" version transmits short pulses where the spaces occur in the "down" beam. If the missile veers too far in the "up" direction, it detects the series of long pulses; if it veers too far in the "down" direction, it detects the series of short pulses; if it is exactly on the midline between the two beams, it detects a steady tone. Left-right position can be conveyed in exactly the same fashion using a different rf carrier frequency or a different pulse repetition frequency. The two schemes described above are not the only possible means of implementing beamrider guidance.

Beamrider guidance is difficult to jam or deceive using self-protection jammers. The rear-facing geometry makes coupling of jamming radiation into the missile guidance an inefficient proposition. The prospects for jamming improve as the missile approaches the target (and the jammer), but the potential miss distance produced by effective jamming decreases as the approach distance decreases. It is often more effective to try to jam the tracking radar that points the beamrider. However, the possibility of electro-optical tracking as an adjunct to the radar may negate the effectiveness of this approach.

Figure G-10. Beamrider missile guidance.



INFRARED GUIDANCE

Passive Non-Imaging Seekers

Reticle seekers are among the earliest proposed infrared guidance techniques and among the most widely utilized. A reticle is a thin optical element coated with a pattern of transmitting regions and non-transmitting regions (the latter may be reflecting or absorbing). Radiation from a target is imaged through the reticle onto a detector. Motion of the reticle pattern relative to the target radiation results in modulation of the transmitted radiation intensity with consequent production of a time-varying photocurrent from the detector. The modulations in the photocurrent carry the guidance error information. The relative motion of the radiation and the reticle pattern is commonly achieved in one of two ways. First, the reticle may be rotated about its center; the radiation pattern and the detector remain stationary. In such a "spin-scan" reticle system, the motion of the reticle transmission pattern through the radiation modulates that radiation. Second, the radiation pattern may be moved over the reticle pattern in a circular fashion by using conical-scanning optics (a rotating tilted mirror or rotating wedge). In such a "con-scan" reticle system, the motion of the radiation pattern over the reticle transmission pattern produces the modulation in the transmitted radiation. Reticles can also be used to produce amplitude-modulated signals or frequency-modulated signals. There are advantages and disadvantages to every combination of scan and modulation formats.

Figure G-11 describes the functioning of a typical spin-scan reticle seeker employing amplitude modulation. In this example, the "rising sun" transmission pattern produces an amplitude-modulated output in which the magnitude of the amplitude is proportional to the distance from the center of the reticle. The neutral (50% transmission) region allows the phase of any amplitude modulation to be determined. When the output from the detector is properly analyzed, the magnitude of the amplitude modulation gives the radial component of target alignment error; the phase of the modulation gives the azimuthal component of the target alignment error. By making appropriate control corrections the amplitude modulation can be driven to zero and the missile is guiding straight at the target.

The rising sun pattern of Figure G-11 was the reticle pattern used in the original Sidewinder missile (AIM-9B) seekers. The seeker locks onto the brightest infrared object in its field of view and tracks it. This worked well when tracking hot exhaust pipes of jet aircraft but ultimately proved susceptible to a variety of countermeasures. The simplest is a small hot flare. If the infrared radiant emission of the flare exceeds the infrared radiant emission of the target (which is generally larger but cooler than the flare), then the seeker will follow the ejected flare. The trend of modern aircraft to have reduced infrared emissions makes this type of seeker even more susceptible to flares.

It is also possible to countermeasure this seeker with modulated infrared sources. Consider a blackbody source large enough and hot enough to have an infrared radiant emission that exceeds that of the target. If a shroud with appropriately spaced transparent slots is placed around this source and rotated at the proper frequency, the emission in any direction will look much like the pattern observed by the seeker at position 1 in Figure G-11. If the seeker looks at such a modulated source, some of the modulated signal will pass through the reticle and be detected at the seeker output. If this modulated source signal is stronger than the normal signal produced by the target, then the seeker will lock onto the modulated source. Since the modulated source acts like a target at the edge of the field of view of the missile, the missile will pull a hard turn in that direction until the target exits the seeker field of view and guidance is lost.

Figure G-11. A typical spin-scan amplitude-modulated reticle seeker and the associated detector outputs at several different target positions.

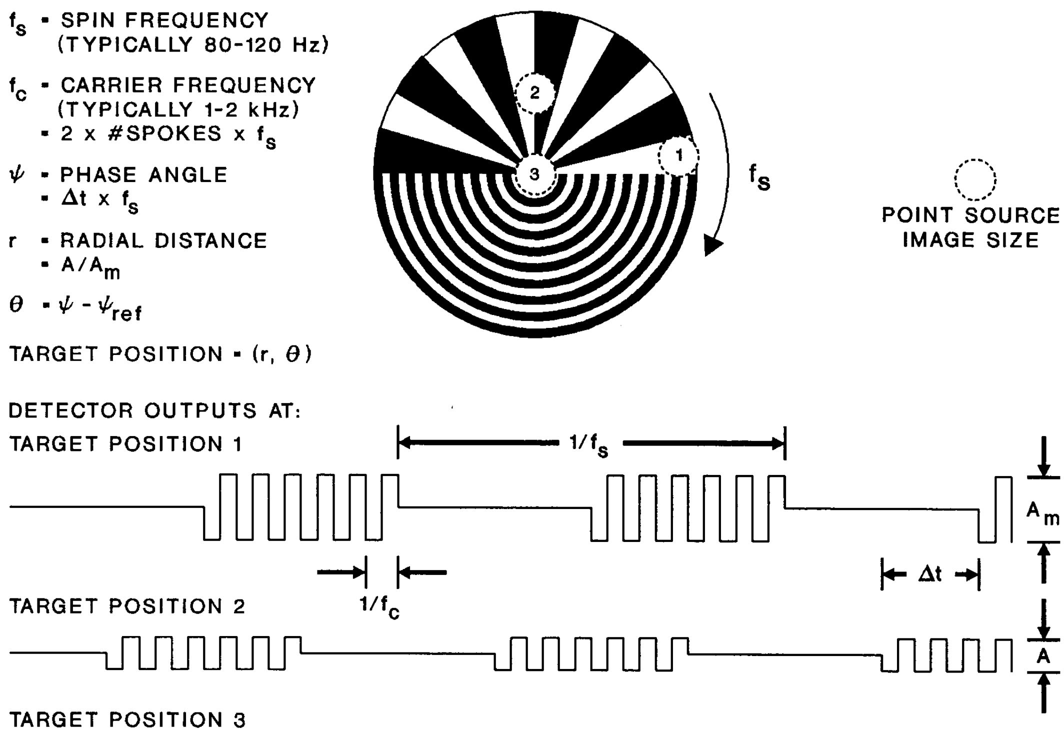
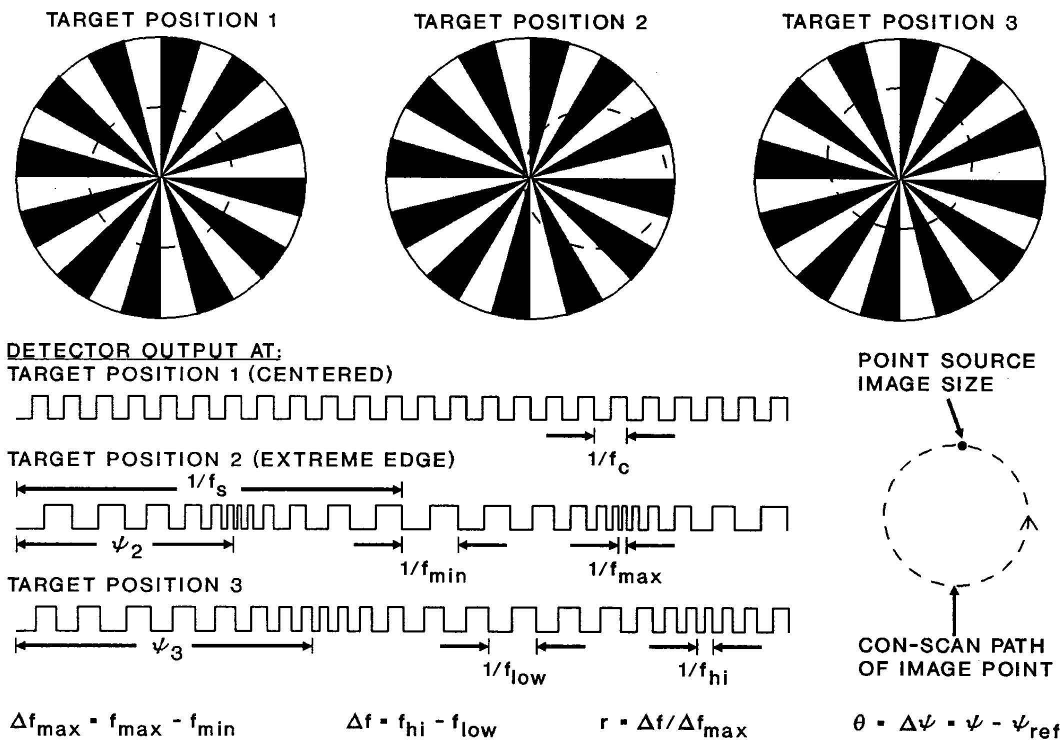


Figure G-12 describes the operation of a con-scan reticle seeker. If the target is located at the center of the field of view, the conical-scanning will move its radiation pattern in a circle about the center of the reticle pattern. The detector photocurrent will have an amplitude modulation at a well-defined carrier frequency. If, however, the target is offset slightly from the center of the field of view, the conical-scanning process moves the radiation in a circle that is offset from the center of the reticle pattern. At some points in the circular scan the radiation pattern takes a long time to traverse a single spoke of the reticle pattern; at other points the traverse time is very short. In this instance, the detector photocurrent experiences a frequency modulation (at times higher than the carrier frequency and at other times lower than the carrier frequency). If the frequency modulation is demodulated by the seeker, the magnitude of the frequency excursion gives the radial component of the guidance error, while the phase of the frequency modulation gives the azimuthal component of the guidance error.

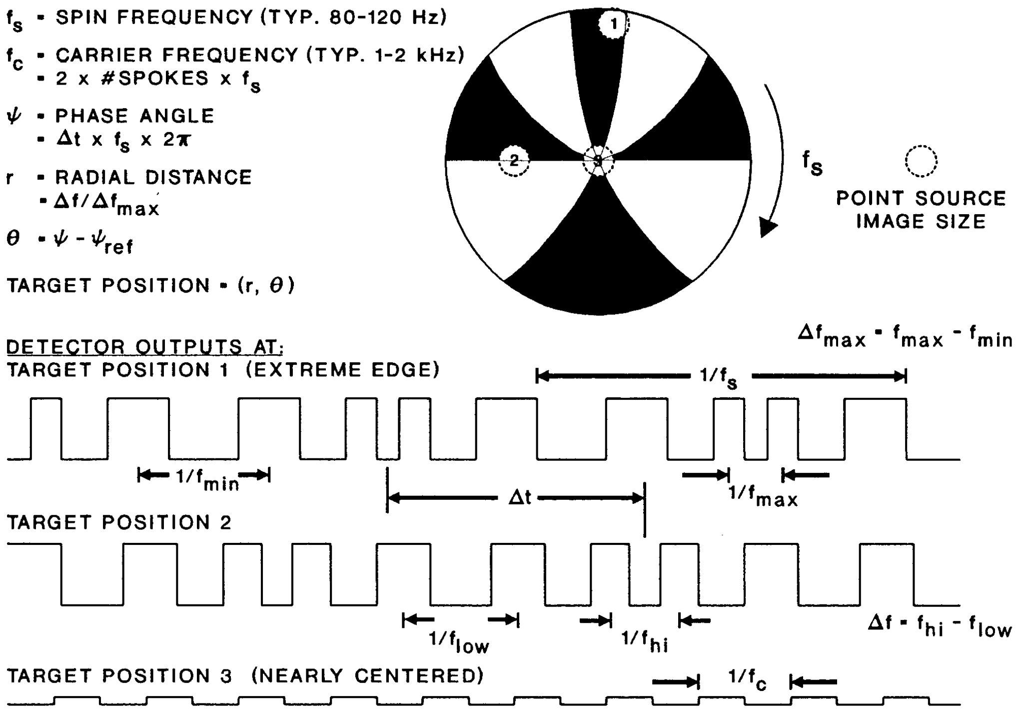
Con-scan FM reticles are somewhat more robust than spin-scan AM reticles in their performance. Some of this derives from conical-scan, the remainder derives from the use of frequency modulation rather than amplitude modulation. Nevertheless, con-scan reticle seekers can be decoyed by flares and can be deceived by modulated infrared jammers of the type described above.

Figure G-12. A typical con-scan frequency-modulated reticle and the associated detector outputs for different target positions.



Spin-scan reticles can also be designed to give frequency modulations as a function of guidance error. Such reticles may be designed from rings of spoke patterns; each successive outward ring having more spokes than the interior rings. As the radial guidance error increases, the amplitude modulation increases from zero to some amplitude at frequency f1. As the error increases further, the amplitude at f1 begins to decrease with a simultaneous increase at frequency f2, and so on. Several spoke sectors may be made neutral to give a time reference, allowing the azimuthal guidance error component may be extracted as a phase angle. Another implementation of a spin-scan frequency modulated reticle is shown in Figure G-13.

Figure G-13. A typical spin-scan frequency-modulated reticle and the associated detector outputs at several different target positions.



Spin-scan FM reticle seekers are arguably no better and possibly less robust than con-scan FM reticle seekers. They can also be decoyed by flares and deceived by modulated infrared sources. However, they do add another dimension to the countermeasure designer's problem. The very possibility of their use must be considered in deception jammer design.

Spectral information is of great use in assisting an infrared seeker to discriminate between the target and countermeasure decoys or thermal clutter. As shown in Figure G-14, targets with skin temperatures around ambient temperature (300 K) have an infrared emission spectrum which is very small at wavelengths below 3 μm and increases rapidly towards a peak near 10 μm. Very hot objects, such as the sun (roughly 5900 K) or a magnesium flare (roughly 2000 K) have their peak intensity below 2 μm and emit very little spectral energy beyond 5 μm. If we measure the intensity in two wavebands (one between 3 μm and 4 μm – such as BAND 1 in the figure – and a second between 4 μm and 5 μm – such as BAND 3 in the figure) then targets will have a ratio of intensity in the two bands

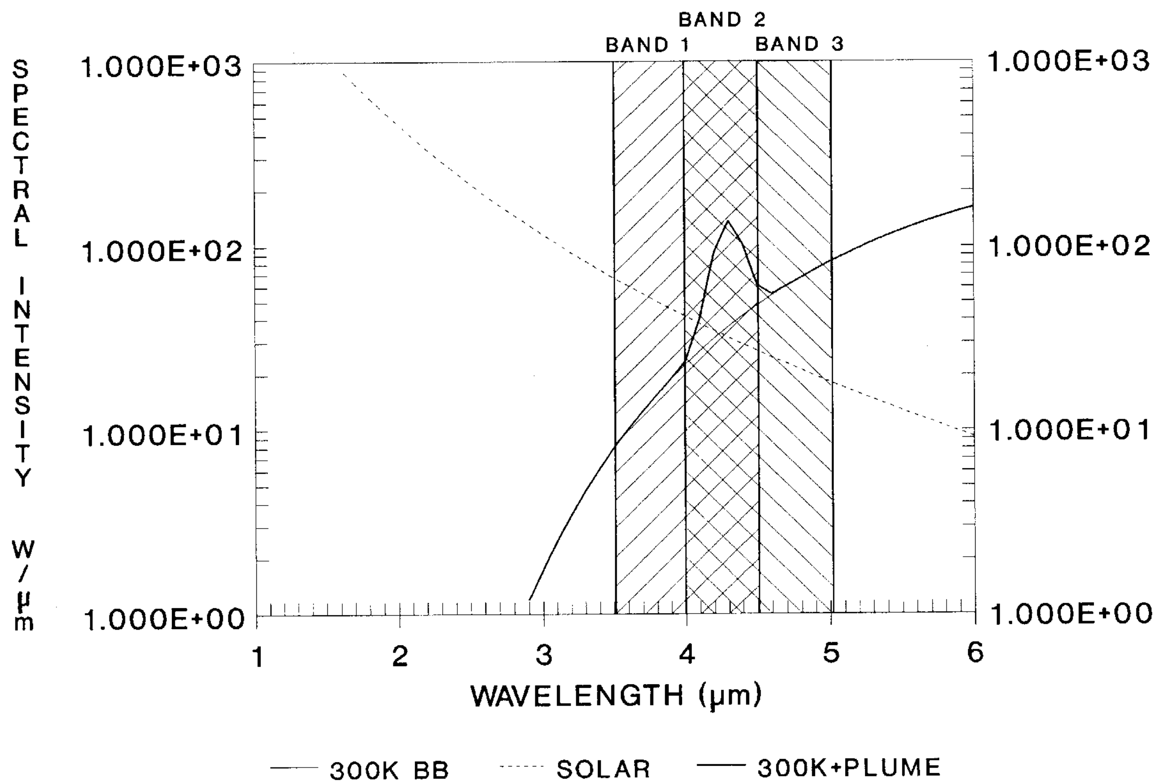
$$BAND\ 1/BAND\ 3\ <\ 1.0$$

while flares, fires, and solar glints (strongly reflected sunlight) will have a ratio

$$BAND\ 1/BAND\ 3\ >\ 1.0\ .$$

The narrow band around 4.3 μm is special. This is the emission line of hot CO_2. Jet engines and the exhaust stacks of large diesel or turbine engines emit plumes containing large amounts of hot CO_2. Addition of a third band (between roughly 4.0 μm and 4.5 μm – BAND 2 in the figure) permits detection of the anomalously large emission from hot CO_2. This provides additional evidence that the object being detected is a target (that often has an exhaust plume as opposed to a decoy or a natural object that does not).

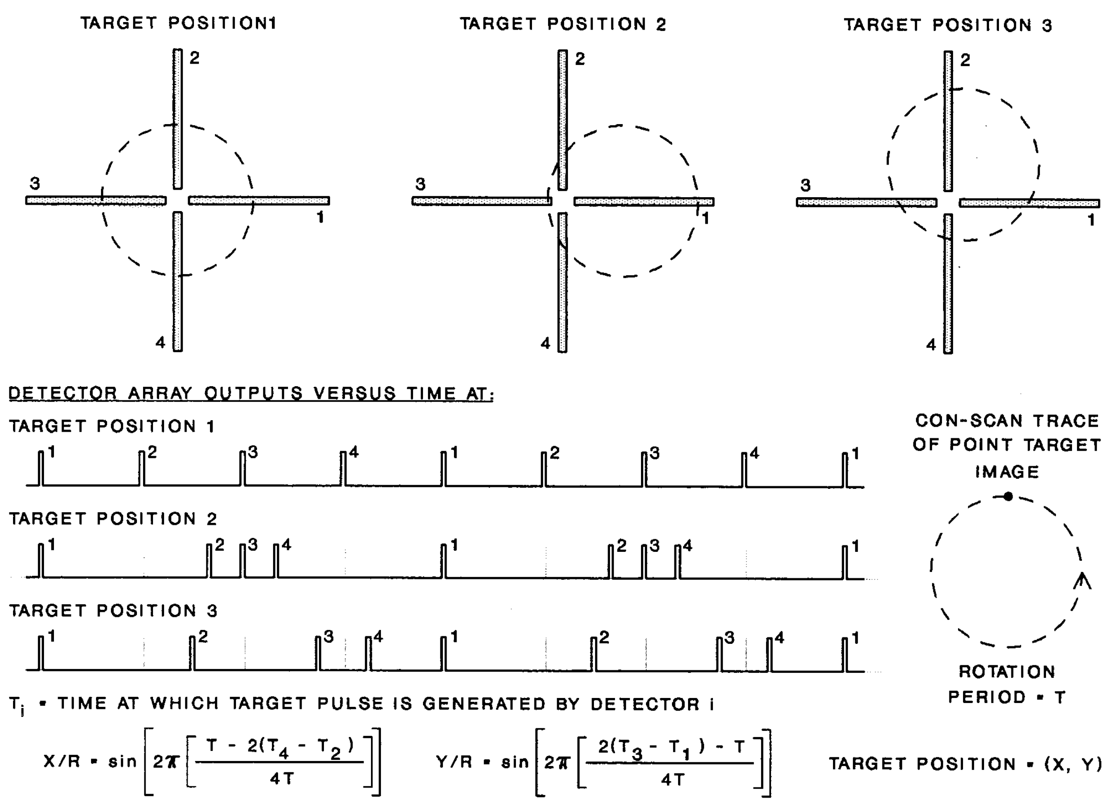
Figure G-14. The principle rationale for multicolor seekers. Hot targets such as the sun have spectral intensities that different dramatically from cool targets. Objects with engine exhaust plumes with exhibit additional emission around 4.3 μm.



By making several reticle patterns out of bandpass filter multilayer coatings, two or more reticle patterns each sensitive to a different waveband may be deposited one on top of the other. A detector looking through such a multi-color reticle will detect two (or more) modulation patterns in the transmitted radiation. The relative amplitude of these modulation patterns provides information on the spectral distribution of radiation coming from the target. Such multi-color reticles are commonly employed as counter-countermeasures against flares. Reticle systems usually are limited to only two wavebands. However, imaging seekers (to be discussed below) may have three or more wavebands, possibly including the CO_2 emission band. With laser-based deception jammers it is conceptually possible although difficult to overcome the counter-countermeasure capabilities of multi-color non-imaging seekers.

A guidance mechanism related to reticle seekers is the **con-scan cross detector array**, as illustrated in Figure G-15. Four long, narrow detectors are arranged in a symmetric cross pattern. Radiation from the scene is conically scanned around the center of symmetry. As radiation from a target scans across each detector, that detector will emit a pulse of photocurrent. If the target is centered in the field of view, each pulse will be equally spaced from its neighbors. If the target is displaced from the center of the field of view, the pulse spacings will be unequal. Appropriate mathematically analysis of the pulse timing (outlined at the bottom of Figure G-15) provides both the horizontal and vertical displacements from the center of the field of view.

Figure G-15. Principle of the con-scan cross detector array seeker.

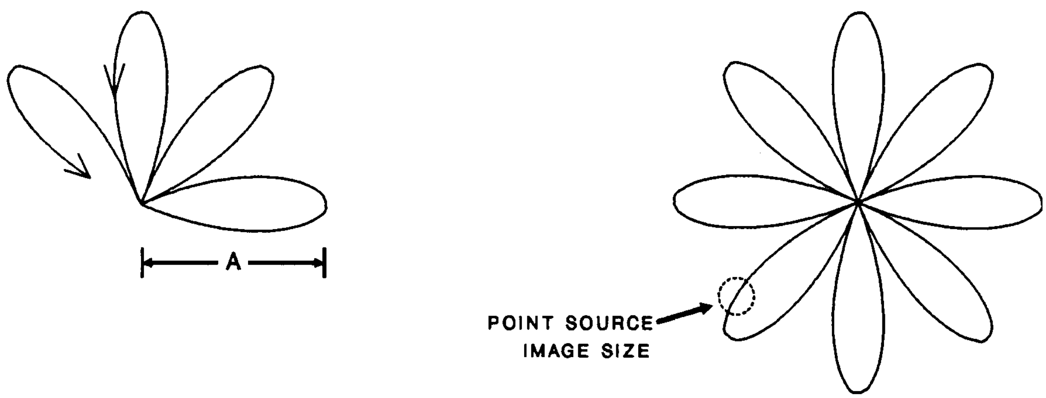


Con-scan crossed array detectors are also susceptible to being decoyed by flares and to being deceived by modulated IR sources. However, like spin-scan FM reticles, their very existence complicates the countermeasure designer's task.

Passive Quasi-Imaging Seekers

By combining a linear sinusoidal scan with a continuous rotation, a **rosette scan** pattern may be generated (see Figure G-16). The rosette patterns are usually chosen to be closed form figures that provide moderately uniform coverage of a circular field of view. Because the coverage is dense enough to produce a coarse image of the field of view, if the data were properly scan-converted, rosette scan seekers are often referred to as pseudo-imaging seekers. As the rosette scan optics move the target radiation across the detector, a brief pulse of photocurrent will be generated. The timing of this output pulse relative to some reference provides both the azimuthal (azimuthal variation is a linear function of the pulse time relative to the reference) and the radial (radial variation is a sinusoidal function of the relative timing) guidance errors.

Figure G-16. Principles of rosette scanning.



ROSETTE PATTERN (T = PATTERN REPETITION PERIOD)

$$R = A \cos n\theta = A \cos 2\pi nt/T$$

n = EVEN INTEGER (PATTERN HAS 2n LEAVES)

n = ODD INTEGER (PATTERN HAS n LEAVES)

PATTERN CAN BE PRODUCED BY COMBINING A LINEAR SINUSOIDAL SCAN WITH A CONTINUOUS ROTATION

PHASE ANGLE IS LINEARLY PROPORTIONAL TO TIME

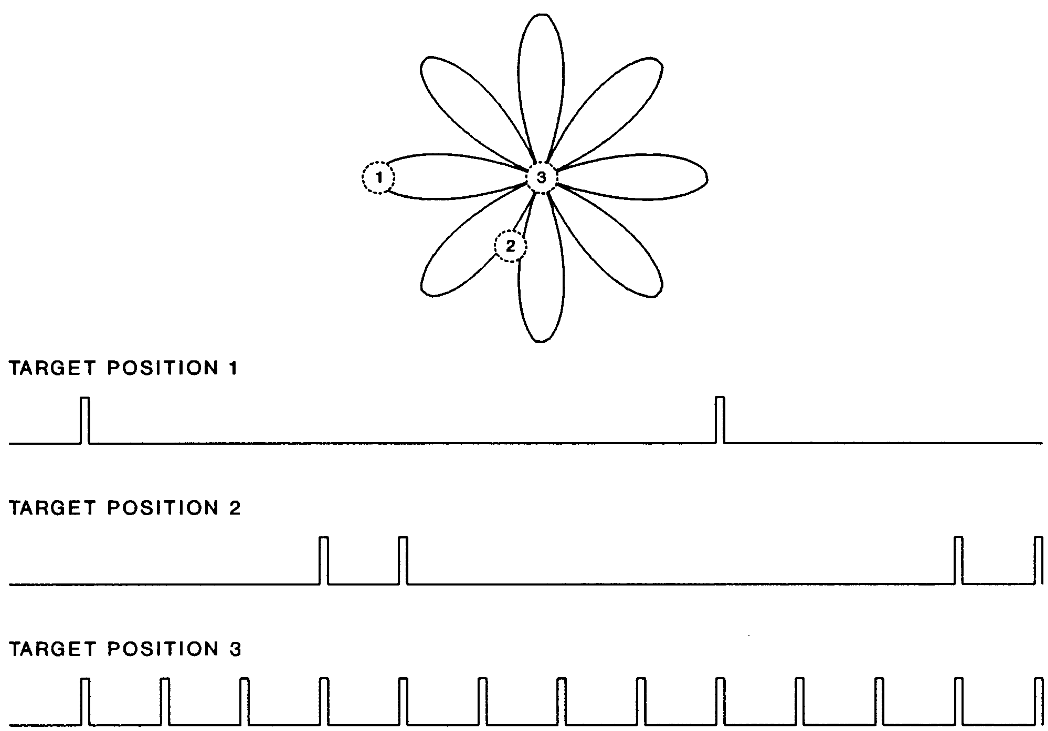
$$\theta = 2\pi t/T$$

TARGET LOCATION = (R, θ)

At the edges of the field of view only a single leaf of the rosette will pass over the target image (see Figure G-17). Here a regular train of pulses will be generated with the pulse period being the rosette pattern repeat time. As the target moves closer to the center, two consecutive leaves of the rosette will pass over the target image. The resulting pulse train now exhibits two closely spaced pulses, repeating at the rosette period. At the very center of the field of view, every leaf of the rosette passes over the target image and a regular pulse train of pulses separated by the leaf period is produced. The transition from double pulses to continuous pulses occurs in integer increments as the target gets nearer the center of the field of view. This fact must be considered in the design of a rosette scan countermeasures system.

Spinning linear array seekers use a linear detector array that is rapidly rotated either about one end or about the center. In this fashion a circular field of view defined by the array length may be completely covered at the rotation rate (or twice that rate if rotated about the center of the array). Radial guidance error is readily obtained from the detector that detects the target radiation. Azimuthal guidance error is determined by the time of target detection relative to a nominal rotation reference time. In one variant of this kind of seeker, the detector array is rotated behind stationary optics. In a second variant, the detector array is stationary, and the image scene is rotated by a prism or mirror assembly (such as a K-mirror). In a third variant, the detector array is stationary, and the image scene is conically scanned about it.

Figure G-17. Electrical waveforms resulting from rosette scanning.



All of the non-imaging infrared seeker techniques described above are susceptible to infrared countermeasures. A variety of techniques can give them some degree of resistance to countermeasures, but ultimately the countermeasure designer has won. For this reason, most future infrared seeker designs will use imaging techniques. These are described in the next section.

Passive Imaging Seekers

The remarkable performance of infrared imaging systems in target detection and weapons delivery has almost assured that the next generation of infrared seekers will use infrared imaging. Figure G-18 depicts the five general types of infrared imaging systems. All five types have been used in on or another thermal imager in the past two decades. The simplest is the one-detector raster-scanned system. The output of the detector is raw video that can be processed or output to a display. One-detector systems generally suffer from poor sensitivity, as the ratio of detector angular size to field of view size is generally very small.

Serial scan systems improve sensitivity by utilizing a number of detector elements to view the same scene point one after another. With an appropriate delay between each of the signals, the sum of all the detector outputs at any point in time represents the sum of all signals detected from a single point in the scene. Time-delay-&-integration (TDI) as this approach is called improves signal to noise ratio by the square root of the number of detectors in the array. Typically, TDI results in this degree of improvement for detector array sizes between 4 and 16. Larger arrays seldom exhibit this degree of improvement due to problems in assuring that the scan process (including any missile or target motion effects) brings the signal across each detector in turn with the proper time delays.

Figure G-18. Detector types used in passive electro-optical imaging systems.

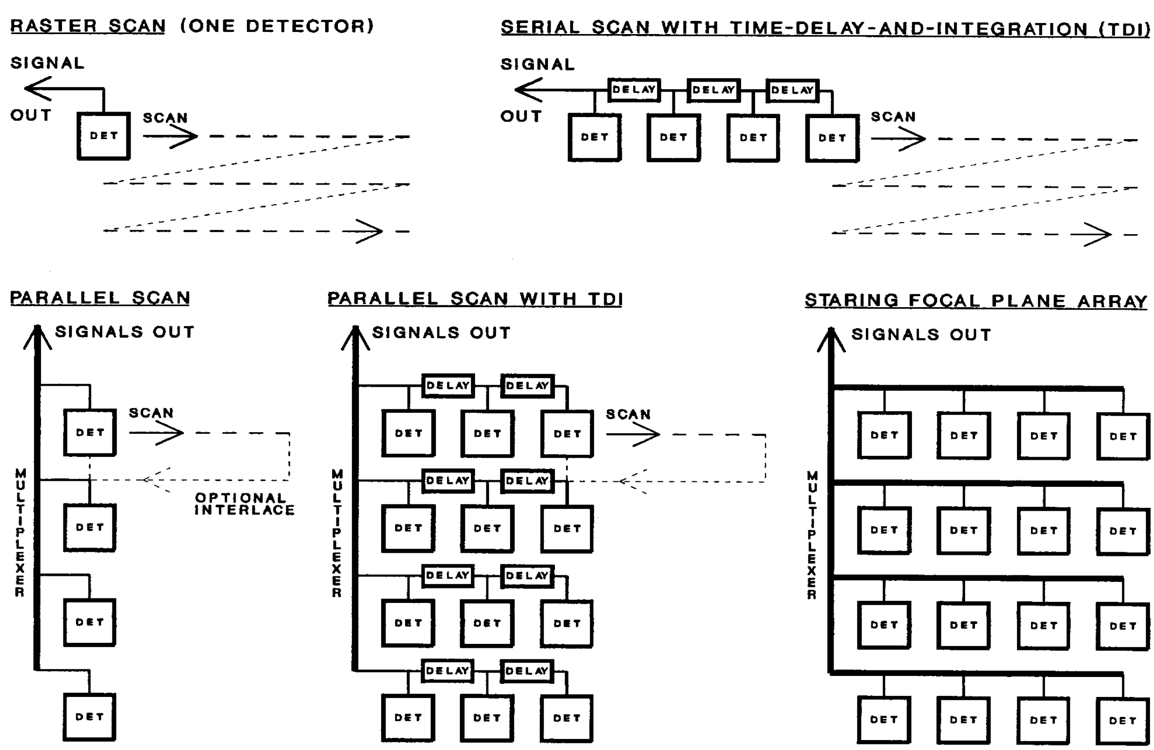


Figure G-19 shows the geometry of a TDI array. Physically and mathematically the output current from a TDI array is given by

$$i(t) = i_N[t; x_N(t)] + i_{N-1}[t-T; x_{N-1}(t-T)] + \ldots + i_1[t-(N-1)T; x_1(t-(N-1)T)] ,$$

where i_n is the contribution to the total current from detector n. For a linear scan, the spatial position viewed by detector n is

$$x_n(t) = Vt + (N-n)L \qquad \text{if} \qquad X_N(0) = 0,$$

where L is the distance between detector elements and V is the velocity at which the image is scanned across the detectors. If $V = L/T$, i.e., the scan velocity is matched to the delay and the detector spacing, then

$$x_n(t) = V[t+(N-n)T] = x_N(t+(N-n)T) \qquad \text{or} \qquad x_n(t-(N-n)T) = x_N(t)$$

For this matched scan the total output current is given by

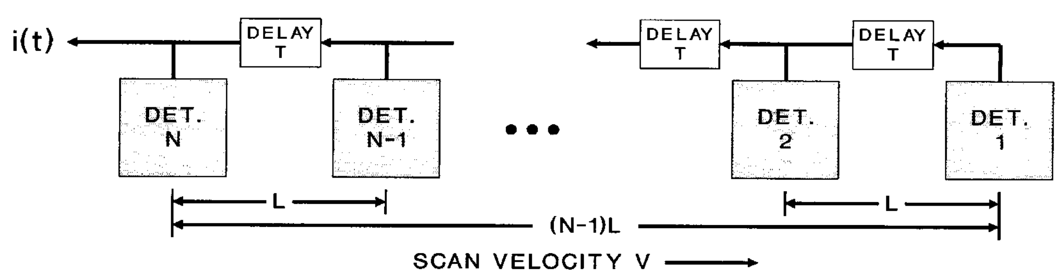
$$i(t) = i_N[t; x_N(t)] + i_{N-1}[t-T; x_N(t)] + \ldots + i_1[t-(N-1)T; x_N(t)] .$$

The output signal is thus seen to be the sum of N components originating from a single point. However, the noise from each detector is uncorrelated with the noises from the other detectors. As a consequence,

$$SIGNAL\ \%\, N \qquad NOISE\ \%\, (N)^{1/2} \qquad SNR = SIGNAL/NOISE\ \%\, (N)^{1/2} .$$

TDI results in a signal-to-noise ratio (SNR) that improves as the square root of the number of detectors being integrated together.

Figure G-19. Geometry of time-delay-and-integration (TDI).



Parallel scan imagers use a long, linear array of detectors to cover one dimension of the field of view (or a small-integer submultiple of that field of view) instantaneously. The array is scanned back-and-forth in the other dimension to generate the image. The output of each detector forms one line of the image. It is not uncommon to butt two or more arrays with different wavelength response side by side at the focal plane. In this fashion multi-color images can be easily obtained.

The fourth type of imager combines the SNR improvement available from TDI with the short frame times available from parallel scan systems by using a specially designed two-dimensional detector array.

Staring focal plane array imagers provide a separate detector element for each picture element (pixel) in the image. These systems provide significant advantages over any of the other 4 types by having the highest sensitivity (radiation may be integrated for the complete time to generate a single frame of image data) and the lack of moving parts (scanners) with their notoriously poor reliability impacts. On the other hand, it is difficult to obtain focal plane arrays of very large numbers of detectors in some wavelength regions. If arrays are available, they may be prohibitively expensive for one-shot applications such as missile seekers.

Multi-color staring focal plane array seekers may be implemented in two fashions. The simplest is to split the signal into its spectral components using dichroic beamsplitters and place a separate focal plane array at the focus of each waveband. Such systems may have cooling problems, alignment problems, or large size problems in seeker applications. The second approach is to fabricate one detector array on top of another detector array. Often a material is transparent at the wavelengths to which it is not sensitive. Such stacked arrays have been demonstrated in the mid- infrared using GaAs quantum well detectors with very promising results. The second approach eliminates the problems of the first, but is still in the early stages of development.

Imaging infrared seekers possess enormous countermeasure resistance. The high resolution possible with infrared imagers means that targets have significant spatial extent. Aircraft look like aircraft, tanks look like tanks, and ships look like ships. Small hot decoys like flares look like small hot decoys. Deception jammers look like blinking "black boxes". But even when decoys or deception jammers are present, targets look like targets. Virtually all currently deployed countermeasures will be ineffective against advanced infrared imaging seekers. Infrared countermeasures to imaging seekers must either be based on precision replicas (decoys that have the same size, shape, and appearance as real targets) or on blinding countermeasures (blooming or saturating the detector outputs or even damaging the individual detector elements). Precision replicas are only practical for ground vehicular targets. Blinding countermeasures require moderate to high-power lasers with precision pointing and tracking and will be very expensive.

Semi-active Laser Seekers

Semi-active laser guidance is completely analogous to semi-active radar guidance. The primary difference is that laser radiation replaces microwave radiation. In semi-active laser guidance, a modulated laser beam is directed onto the target by a separate fire control system. This fire control system may be a soldier pointing a laser designator by hand, or it may be a sophisticated electro-optical fire control system employing a thermal imager or television for target tracking. Some of the laser radiation reflects off the target and can be detected by a quadrant detector array, placed at the focal plane of a lens system that converts angular position information into spatial displacement information. By taking appropriate sums and difference of the signals from the four elements of the quadrant detector array (see Figure G-6 – a quadrant detector is essentially the same as a monopulse receiver), the horizontal and vertical angular position errors of the target may be detected. Signal-to-noise ratio in semi-active laser seekers is enhanced by placing a narrowband optical filter at the laser wavelength in front of the detector array (to eliminate background optical radiation) and by synchronously detecting the signal at the modulation frequency.

Countermeasures exist to laser semi-active guided missiles, as they do to most guidance systems. High-intensity laser beams can blind the missile seeker. A laser repeater jammer can produce multiple copies of the laser spot at different locations on the ground (this only works for targets that are essentially on the ground). Expendables can be designed to emit laser radiation that looks like the spot on which the seeker is designed to home.

Laser Beamrider Guidance

Laser beamrider guidance is the laser radiation analog of microwave beamrider guidance. In laser beamrider systems, a laser beam is pointed in the direction the missile is to fly. A sensor (or sensors) on the missile interprets the radiation received from the laser beam to determine the missile's distance from the center of the beam. This interpretation can be accomplished in many different ways. If the laser beam is conically scanned about the desired flight direction, the detector on the missile will see an amplitude modulation that increases in strength as the missile moves away from the centerline. On the desired flight path the amplitude modulation is zero. The missile may fly a slightly wobbling path along the laser beam and its sensor can detect the normal off-axis decrease in beam intensity as an amplitude modulation. A hill-climbing servo loop will keep the wobble at a minimum and centered about the beam. The laser beam may be spatially encoded. That is, the transverse beam pattern is divided into small elements, and each element is modulated differently in time. The missile detects the modulation pattern and then knows in which beam element it is located, and can correct its flight accordingly. The laser beam may be raster-scanned over some small solid angle. A clock on the missile is synchronized with this raster pattern. When the laser beam scans over the rear of the missile, the detector will sense a pulse. The time at which this pulse occurs tells the missile where it is in the raster pattern and the missile can then correct its motion. Many other information encoding techniques can be and are used by various laser beamrider systems. A laser beamrider system needs a sensor at the laser platform that tracks the target and points the laser beam at that target. This sensor is usually a moderate to high resolution imaging sensor such as a thermal imager, a television sensor, or possibly a human eye. This fire control sensor does not need to track the missile; the missile is responsible for keeping itself centered in the guidance beam.

The rearward looking receivers on laser beamrider systems are almost impossible to jam. The best countermeasure techniques for countering laser beamrider missiles are to blind the fire control system that points the guidance beam. This will require medium- to high-power lasers (almost certainly at multiple wavelengths as most fire control systems employ several different electro-optical sensors), a high quality target acquisition system (to locate the fire control platform), and precision pointing and tracking (to place the blinding laser beams on the appropriate apertures). Because the fire control sensors do not close with the target (as missile seekers do), jamming the fire control sensors of a laser beamrider will be harder than jamming an infrared imaging seeker.

Command Guidance

Infrared (or electro-optical) command guidance is completely analogous to rf command guidance. In any command guidance system, a fire control sensor (or sensors) detects and tracks the target and also tracks the missile. A processor in the fire control system computes the guidance errors and transmits specific guidance commands (up/down, left/right, how much) to the missile. The missile receives these commands and adjusts its control surfaces accordingly.

In infrared command guided systems, the fire control sensors are typically electro-optical or infrared sensors. Television cameras, thermal imagers, or direct view optics (magnified human vision) are the typically systems used to generate the data for missile and target tracking. The processing necessary to generate guidance error signals may be done by computer, or may be done by a human operator.

The commands from the fire control system may be communicated to the missile in several ways. A radio frequency communication link may be employed, as may a laser communication link. Some missiles dispense a wire as they fly and use this wire to carry guidance commands. A more recent variant of wire guidance is fiber optic guidance. In this case, the missile dispenses a fiber optic cable as it flies. The fiber optic cable carries guidance commands to the missile. In some variants of this class of missiles, the fiber-optic cable may also carry information from a sensor on the missile back to the fire control system, effectively eliminating the need for a sensor at the fire control system. This last type of guidance is more properly an imaging seeker with part of the autopilot displaced from the missile to the launcher.

Countermeasures to many electro-optical command guided missiles will be similar to those required to counter laser beamrider missiles. The exception to this observation is the fiber-optic guided missiles with imaging sensors on the missiles. The countermeasures to these systems will of necessity look like countermeasures to infrared imaging seekers.

Active Infrared Seekers

Active infrared seekers replace the passive sensors on the missile with active sensors, or laser radars. The seeker emits a laser beam that illuminates the target. The back-reflected laser radiation is detected by a sensor and used to determine target position relative to the center of the seeker field of view. Active infrared seekers are perfectly analogous to active radar seekers, except that the infrared "radars" employ much higher frequency radiation.

The laser radar can take several different forms. It may consist of a con-scanned or rosette-scanned laser beam and a simple direct detection receiver that detects the modulations in the back-reflected signal. The seeker converts the modulations to position information in a manner analogous to the corresponding passive seekers. The seeker may or may not extract target range information from the returns. The active seeker may utilize a high-PRF laser and a raster scan mechanism to form an image, with guidance information being extracted from the image contents. The receiver for such an imager may use direct detection or it may utilize heterodyne detection. Coherent reception laser radars such as this last one can produce three-dimensional target images and measure the closing velocity. This gives them the potential for automatic target identification and countermeasures resistance superior to both passive infrared seekers and active microwave seekers. Such seekers have been demonstrated for high value missiles such as cruise missiles and strategic interceptors, and may find application in tactical situations in the near future.

Active infrared seekers will have countermeasure resistance characteristics very similar to passive infrared imaging seekers. Laser based countermeasures that aim to blind the receiver in the seeker will be required.

APPENDIX H. STEALTH

Stealth is the process of reducing all significant observables (emitted or reflected radiation or other signatures that can be detected by an appropriate sensor) of a platform to levels that make it difficult to attack that platform. Critical observables usually include: radar cross section (RCS), infrared emission, rf emissions, visual contrast, acoustic emissions, and magnetic field anomalies. The first five are most important for aircraft; the last two are most important for submarines; and all are important for surface warships. In the following paragraphs we will describe the essential characteristics of stealth at the simplest and totally unclassified level.

Because radars are among the most ubiquitous long-range sensing systems in the atmosphere, most work on stealth involves reducing the radar cross sections of ships and aircraft [64]-[66], [158]. Radar cross section (σ) is the effective size of a target as viewed by a radar. It is a function of three components: physical size (A - affecting how much of the radar beam the target intercepts), reflectance (ρ - affecting how much of the intercepted radiation gets re-radiated), and retrodirectivity (ψ - affecting how much of the re-radiated radiation is directed back at the radar and not elsewhere). That is,

$$\sigma = A \rho \psi .$$

The physical size of a platform is usually determined by payload, range, and speed requirements, so little can usually be done with this factor. The reflectance is a function of the surface materials of the target. Bare metals and many painted metals have reflectances near unity. Some materials will absorb incident electromagnetic radiation (they appear "black" at the appropriate frequencies). By analogy with visible reflectances – most surfaces that appear black actually reflect 1% - 10% of the incident light – we expect that simple absorbing coatings and applique materials (radar absorbing materials) can reduce the reflectance to between 0.01 and 0.1. More complicated composite structures (radar absorbing structures) can achieve lower reflectances but have so much physical depth that they must be designed into the target from the beginning. Retrodirectivity is the degree to which the target reflects radar energy back at the radar rather than scattering it isotropically. Certain geometric shapes preferentially reflect energy back at the radar. For example, a corner reflector (three reflecting planes each at right angles to the other two – a trihedral) will reflect any ray that strikes it back along the exact direction of incidence. This retroreflective character is illustrated in Figure H-1 for two kinds of sources. Other shapes can preferentially reflect energy away from the radar (as shown in Figure H-2). Design for radar stealth is therefore an activity that tries to incorporate good geometric shapes into the design while eliminating all bad geometric shapes, and makes appropriate use of reflectance reducing coatings and structures.

The primary effect of radar cross section reduction is a reduction in detection range. As discussed in Appendix E, the radar CNR will scale proportional to cross section and inversely proportional to the fourth power of range. For a constant CNR, detection range will be reduced by the fourth root of the cross section reduction (i.e., 4 orders of magnitude reduction in RCS will produce a 1 order of magnitude reduction in detection range). This is illustrated in Figure H-3. Reduced detection range means that adversary forces have much less time to react to a low

Figure H-1. Retroreflection a) from dihedrals and trihedrals and b) from antennas.

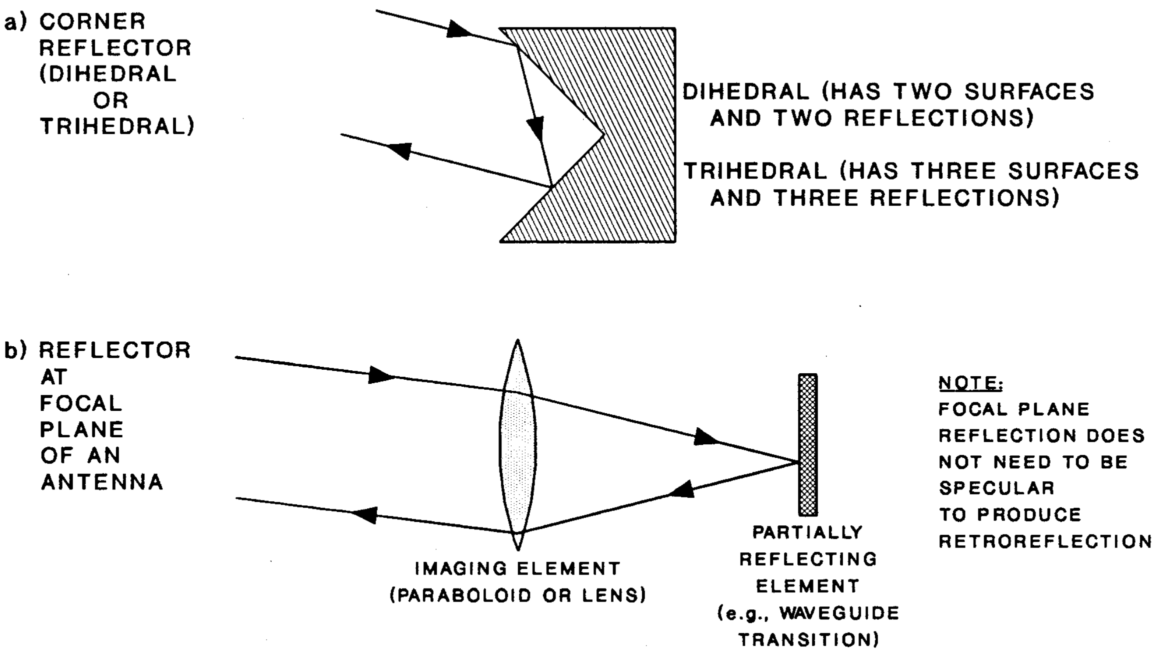


Figure H-2. Use of oriented surfaces to direct radar returns away from threat radars.

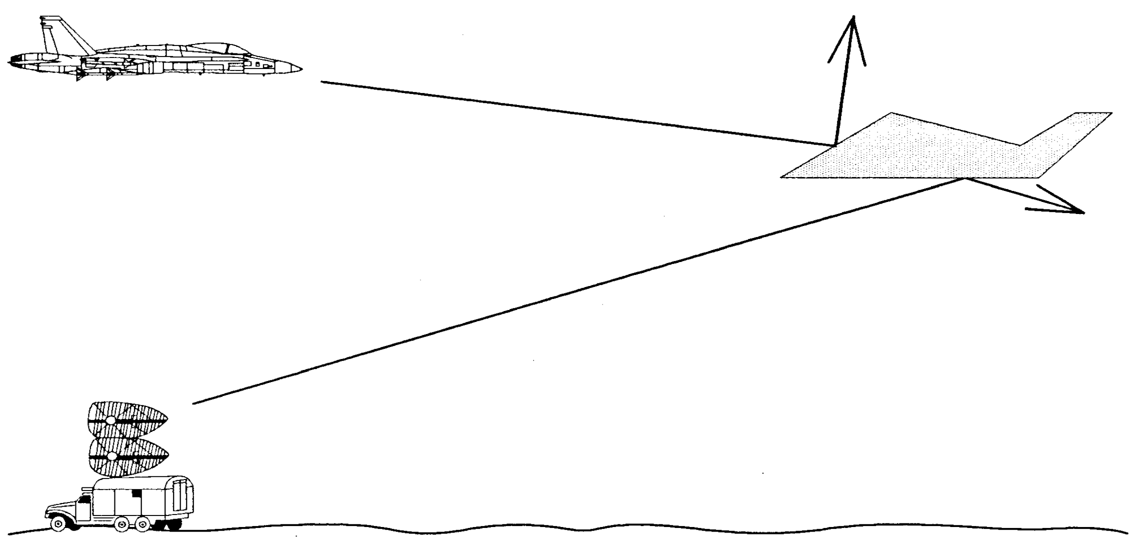
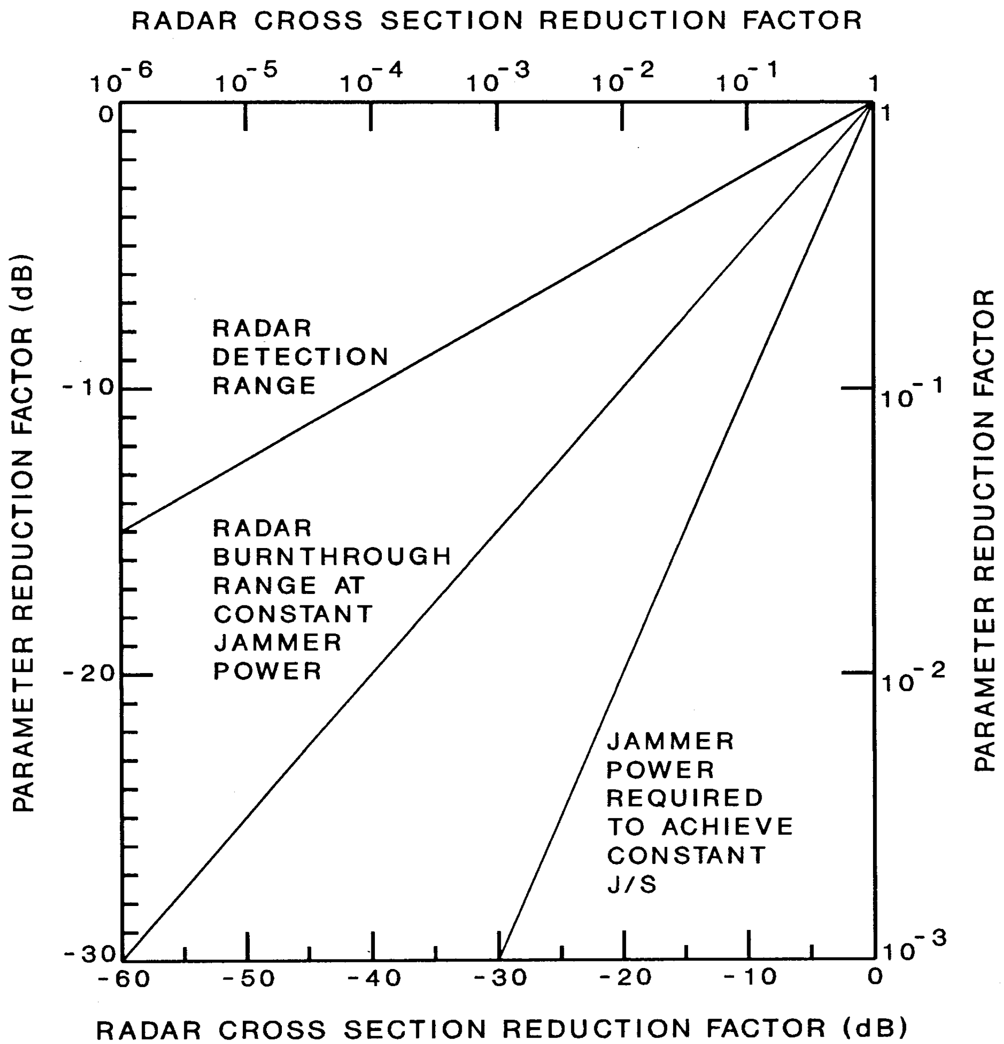


Figure H-3. Effects of radar cross section reduction.



RCS target. The reduction in available reaction time may make it impossible to intercept the low RCS platform. Reduced RCS has two other effects. If the platform carries a jammer, then at some range, a radar attempting to detect the platform in the presence of the jammer, will finally be able to do so. The radar signal grows faster than the jammer signal. The point at which the jammer becomes ineffective is the burnthrough range. Reduced RCS reduces the burnthrough range as the square root of the RCS reduction for a constant power jammer. If at a fixed range, the jammer is required to produce a given jamming-to-signal ratio, then the jammer power required is reduced by the same amount as the RCS is reduced. Although a modest amount of radar stealth may have a small reduction on detection range, it can permit greatly reduced jammer powers to be effective. This has a significant cost, weight, volume, and power benefit to the reduced RCS platform.

The infrared signature of a target is the contrast of the target's thermal emissions (plus any reflected infrared) against the thermal emissions (plus reflected radiation) of the background, i.e.,

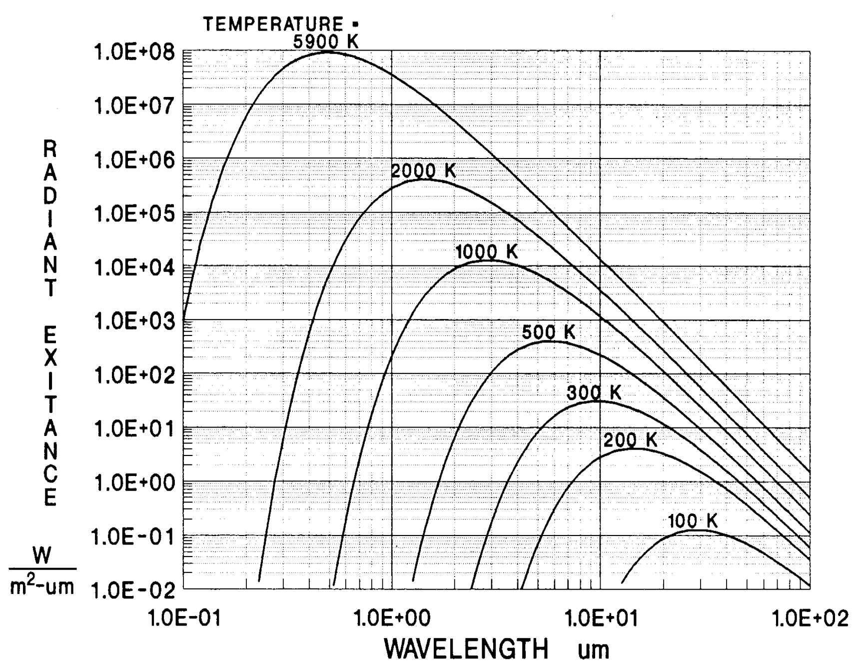
Contrast = ((TGT radiation – BKG radiation)/(TGT radiation + BKG radiation))

The thermal emission (or spectral radiant exitance) of any surface is given by the Planck distribution:

$$M_\lambda \text{ (in W/m}^2\text{-}\mu\text{m)} = 3.74 \times 10^8\, \varepsilon_\lambda / \lambda^5\, [e^{14388/\lambda T} - 1]$$

where λ is the infrared wavelength, ε_λ is the spectral emissivity of the target, and T is the temperature. Figure H-4 illustrates the wavelength and temperature behavior of the Planck distribution. The emissivity of a surface is one minus any transmittance or reflectance. A perfectly absorbing surface has an emissivity of one. If the intensity of target radiation exactly matches the intensity of the background radiation, then the target will have no contrast against that background and the target will effectively disappear. Infrared stealth attempts to make the target temperature and spectral emissivity match those of the background. Since many targets can be considerably hotter than the background, most efforts go into reducing the temperature of the viewable target surface. Masking hot surfaces by placing colder surfaces into the line of sight to a presumed infrared sensor or seeker, is a commonly employed practice. The introduction of multicolor or even hyperspectral infrared imaging systems has complicated the problem of infrared stealth. At its ultimate, infrared stealth must address matching the infrared brightness, infrared color (spectral variations), and infrared texture of target and background, just as described in the next paragraph on visual stealth.

Figure H-4. The Planck distribution.



The visual signature of a target is the contrast of target reflected light against background reflected light for each resolvable element (pixel) of the image. Most targets do not emit visible radiation of their own (except possibly at night). The reflected light at any wavelength is usually a simple product of the illumination intensity and the reflectivity of the surface. Because of the higher resolution of visual sensors, visual signature must consider not only overall brightness, hue (color), and saturation (degree of white admixed into the hue) of the reflection but also the texture. Texture is a correlated spatial variation in intensity or color across a target or background, i.e., uniform vs. striped vs. mottled vs. checkered vs. spotted, etc. Visual stealth (also called camouflage) attempts to make the target surface match the color, brightness, saturation, and texture of the background. It also requires control of any visible emissions (lights).

The acoustic signature is the sound emissions produced by vibrations of the target or the medium in which the target moves. These emissions contain broadband noise components as well as variable tones (single frequencies) and harmonics. Aerodynamic (hydrodynamic) flow, rotating or reciprocating machinery, and people are common sources of acoustic signature. Acoustic stealth attempts to reduce the emissions by reducing the amplitude of vibrations at their source (by balancing rotating equipment, for example) and damping out, absorbing, or canceling the remaining vibrations before they reach the exterior of the target and propagate into the surrounding atmospheric or oceanic medium.

The rf signature is the radio frequency (and microwave) equivalent of the acoustic signature. rf emission stealth is attempted by EMCON (emission control – turning off rf emitters that are not essential), good electromagnetic interference practices (elimination of electromagnetic noise), and use of low probability of intercept transmitters (wide-bandwidth spread spectrum signals, controlled directional transmission with narrow beamwidth and low sidelobes, and minimum output power).

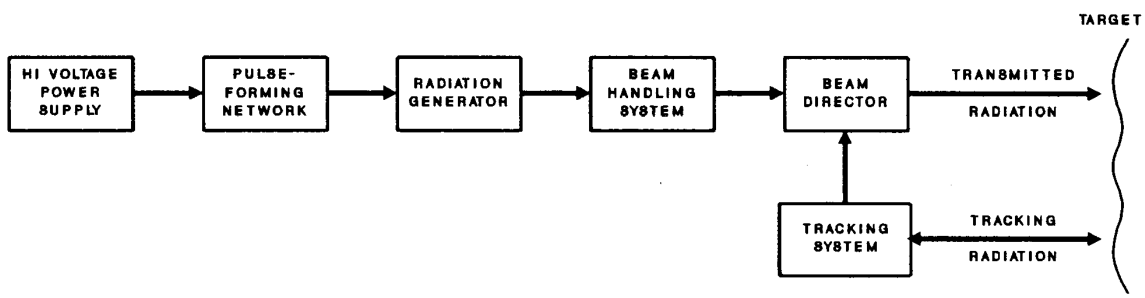
The magnetic signature is the difference between the magnetic field surrounding a target and the Earth's magnetic field (in the absence of the target). It consists of an eddy current contribution, a permanent magnetization, and a dipole magnetic anomaly. The eddy current magnetization is produced when any conducting object moves through the Earth's magnetic field. Any ferromagnetic object may gradually acquire a permanent magnetization simply by remaining stationary in the earth's magnetic field – thermal excitation gradually causes some of the ferromagnetic domains to align with the field (a condition of lower energy). The magnetic anomaly is a distortion in the Earth's magnetic field produced instantaneously by any ferromagnetic shell (such as a ship's hull), because magnetic field lines tend to concentrate in the shell rather than in the surrounding non-ferromagnetic space. Magnetic stealth involves designing systems without ferromagnetic components (e.g., all titanium, aluminum, or plastics) and degaussing the object using multiple orthogonal current-carrying coils that produce fields exactly opposite and canceling the static magnetization (and if made possible by addition of extra field sensors, the motional magnetization).

APPENDIX I. DIRECTED ENERGY WEAPONS

Directed energy weapons (DEW) [81] include high-energy lasers [80], high-power microwaves [76], and electromagnetic radiation countermeasures [159]. Work performed in the 1970's and 1980's studied the potential utility of x-ray lasers (pumped by nuclear explosives) [160] and high-power electron beams, proton beams, positive-charged and negative-charged ion beams, and neutral particle (atomic) beams [80], [81]. None of these particle beam systems could be made to propagate interesting distances (kilometers) through the atmosphere and only x-ray lasers and neutral particle beams could be used in space. Interest in these technologies for weapon applications has diminished significantly. They will not be discussed further. Only devices emitting electromagnetic radiation in the optical (visible and infrared) or microwave portions of the electromagnetic spectrum appear to be of practical use as directed energy weapons.

Almost all practical, directed energy devices have the same basic architecture, as shown in Figure I-1, although specific systems may delete one or more of the following major components. A power supply generates, stores, and/or conditions energy (usually electrical) for use in the weapon. A pulse-forming network shapes the energy release into a pulse of proper amplitude and time duration. A radiation generator (a laser or a microwave tube) converts the incident energy into electromagnetic radiation. A beam director system (usually a steerable antenna for microwave systems or a pointable telescope optical system for laser systems) transmits the radiation in the direction of the target. A beam handling system transports the radiation from the generator to the beam director and conditions the beam for proper propagation. Finally, a tracking system is needed that tracks the target and controls the aimpoint of the beam director.

Figure I-1. Block diagram of a generic directed energy weapon.



In general we may classify practical DEW into two categories: optical and microwave. Optical DEW invariably uses lasers as radiation sources. With the exception of free-electron lasers, all laser systems involve pumping electrical, optical, or chemical energy into an ionic, atomic or molecular medium [161]. The pump energy kicks the ionic, atomic, or molecular species into an excited energy state. If the proper species has been chosen and the pump energy is large enough, then more of the species will be in an excited state than in some lower-lying energy state. This is the process of population inversion. When an inversion exists, the normal process of absorption is reversed. If radiation (having a frequency matched to the energy difference between the excited and lower-lying states) is incident on a normal population (more species in the lower-lying level), then more radiation will be absorbed (forcing the species from the lower state to the upper state) than is emitted (allowing the species to drop from the upper state to the lower state). If the radiation is incident on an inverted population, then more emission occurs than absorption. The inverted population produces optical gain. Optical radiation passing through the medium will be amplified. It is well known from electronics that any amplifier can be converted into an oscillator if it is placed into a feedback circuit in which the amplifier gain exceeds the circuit losses. By placing the inverted population between two mirrors, optical feedback can be established, and an oscillator (called a laser – light amplification by stimulated emission of radiation) is created.

For use in a directed energy weapon, a laser must be capable of emitting large powers or pulse energies while sustaining reasonable efficiencies in consumption of pump energy. Several species have proven of interest. Carbon dioxide (CO_2) lasers emit at many wavelengths between 9 and 11 μm although its strongest emission is at 10.59 μm. They can be pumped by electric discharges or by gasdynamic processes (expanding and cooling hot carbon dioxide from a "rocket engine" through a supersonic nozzle will produce an intense inversion) [162]. A gasdynamic carbon dioxide laser was used in the Air Force's Airborne Laser Laboratory (ALL) which demonstrated an ability to shoot down a guided missile in flight from an airborne platform [79]. Although carbon dioxide lasers cannot produce the highest power levels needed for ballistic missile defense, lower power systems can be used to countermeasure infrared seekers. Hydrogen fluoride and deuterium fluoride lasers produce inversions from the chemical energy released when fluorine gas reacts with hydrogen (deuterium) [163]. Hydrogen fluoride (HF) lasers emit at many wavelengths between 2.6 μm and 3.0 μm. Although these wavelengths are strongly absorbed by the atmosphere, HF lasers are serious candidates for space-based defense systems. Deuterium fluoride (DF) lasers emit at many wavelengths between 3.6 μm and 4.0 μm. DF laser wavelengths propagate well through the atmosphere. The MIRACL laser at the High Energy Laser System Test Facility (HELSTF) at White Sands is a DF laser. The primary drawbacks to DF lasers are the high cost of the deuterium fuel and the difficulty in environmentally safe disposal of the toxic byproduct (i.e., DF itself). The Chemical Oxygen Iodine Laser (COIL) uses a chemical reaction to produce excited oxygen molecules which subsequently react with iodine molecules to produce excited iodine atoms (the lasing species). The COIL laser emits at a wavelength of 1.315 μm. This wavelength propagates well through the atmosphere at high altitudes, but has enough absorption (due to water vapor) at low altitudes to make its utility questionable at sea level. The Air Force is using a COIL device in their new airborne laser (ABL) ballistic missile defense system [85]. The ABL flies at high altitudes and shoots at missiles as they leave the atmosphere, so the water vapor absorption is not a problem.

Free electron lasers operate on an entirely different principle [87]. Relativistic electrons are passed through a region of spatially alternating magnetic field polarity (N up, N down, N up, N down, etc.) produced by a large number of strong magnets with alternating orientation. This device (called a wiggler) causes the electrons to alternately be bent one direction and then the other in a periodic fashion. The accelerations produced by this periodic wiggling cause the electrons to emit electromagnetic radiation (accelerated charges radiate!). Because the wiggling is periodic with a fixed frequency, the emitted radiation will have that same frequency. By placing mirrors for feedback on opposite ends of the wiggler, laser oscillation can be made to occur.

Free electron lasers have the potential to efficiently produce very high-power coherent radiation that can be tuned to any desired wavelength. At the present time, output powers useful for missile defense have not yet been demonstrated and free electron lasers are too large for military applications. However, it is reasonable to expect that these limitations will be overcome in the next twenty years and free electron laser-based weapons will be available.

Microwave radiation sources are invariably electron tubes that operate somewhat similarly to free electron lasers. In almost any microwave tube, high voltage electrons emitted from an electron gun interact with the tube structure, with external electric and magnetic fields, and with self-induced fields in a fashion that results in current oscillations at microwave frequencies. The oscillating currents emit microwave radiation. There are many different kinds of tubes using different structures and field configurations that are capable of producing intense microwave outputs. The reader is referred to the text by Benford and Swegle [76] for details of tube design and the physics of tube operation. Currently, tubes can be obtained at any frequency between 500 MHz and 50 GHz with peak powers as high as 1 to 10 GW. At the present time practical HPM weapons capable of destroying shielded electronics can be built that work over relatively short ranges (hundreds of meters). Long-range systems (tens to hundreds of kilometers range) await major improvements in tubes and power supplies. Tube technology has long been capable of supporting jamming systems at microwave frequencies, as the output power requirements for jamming sources are in the kilowatts to megawatts as opposed to gigawatts to terawatts.

All directed energy weapons function by directing electromagnetic radiation onto a target at sufficient power density for a sufficient period of time to create a desired effect. The maximum power density that any directed energy weapon can produce at a target is given by

$$I \cong 4\, P\, D^2\, e^{-\alpha R} / \pi\, \lambda^2\, R^2$$

where P is the transmitted power, D is the diameter of the transmitting aperture, α is the atmospheric attenuation (often negligible), λ is the wavelength of the radiation, and R is the range from the transmitter to the target. The power density from real systems can actually be up to 30% larger or smaller than that predicted by this expression, depending on the exact shape of the aperture illumination function. Uniform illumination will produce roughly 30% less power density. Gaussian illumination will produce roughly 30% higher power density.

If λ/D is much less than 1 mrad, then aimpoint jitter due to platform vibrations may significantly move the beam around its long-term average centroid on millisecond time scales and smear out the energy deposition. Inertial stabilization of the beam can reduce jitter effects to acceptably small levels. Inertial stabilization involves measuring the angular motion of the platform using gyroscopes followed by compensating reverse angular motion of the beam pointing system. Stabilization to residual motions as small as tens of microradians is commonplace. Stabilization to sub-microradian residual motions is challenging but demonstrable.

At visible and infrared wavelengths, atmospheric turbulence can have a similar smearing effect. Turbulence smearing has two major components: beam wander (which occurs on fractions of a second time scales) and beam spread (an instantaneous distortion of the beam that changes randomly on millisecond time scales). The majority of this smearing is due to phase aberrations imparted to the beam due to the fluctuating atmospheric refractive index produced by randomly moving “blobs” of air (officially called turbules) of random sizes located between the laser and the target. Turbulence smearing can be reduced to insignificant levels if not completely eliminated by using adaptive optics. If the adaptive optics imposes the phase conjugate of the turbulence aberration on the beam, then when the phase conjugate beam propagates to the target, the turbulence adds the normal phase aberration to the conjugate phase, resulting in nearly complete cancellation. The result is a smooth beam with maximum power density. An adaptive optical system is composed of a wavefront phase sensor (that measures the spatial distribution of the phase aberration imposed on a signal reflected from the target) [164] and a deformable mirror (that warps its surface in response to two-dimensional electrical inputs to impose the conjugate phase profile on the transmitted laser beam) [83]. Due to growing use by the astronomical community, adaptive optics has become a relatively mature technology and will be a part of almost any system employing laser transmission through the atmosphere.

Thermal blooming is caused by absorption of a small portion of the laser radiation by the air itself. This absorption heats the air and causes it to undergo thermal expansion. The resulting density reduction is greatest near the center of the beam. Since refractive index is a linear function of density, the expansion forms a negative (diverging) lens. The negative lens of the heated atmosphere causes the beam to expand rapidly. The expansion of the beam significantly reduces the power density at the target. Adaptive optics can partially (but not completely) compensate for thermal blooming by imposing an additional focus to the initial radiation. However, the residual beam divergence from compensated thermal blooming may often be too large for weapons applications. Choosing a wavelength with minimum absorption and resulting minimal thermal blooming is much more beneficial.

Directed energy weapons can produce a variety of effects. In order of increasing required power density these can include:

- noise injection into a receiver
- overload of receiver amplifier circuits
- electrical burnout of receiver components
- direct thermal damage of primary receiver elements
- damage to optical components
- melting and structural failure of domes or bodies.

The desired effect occurs when the incident radiation exceeds the threshold for that effect. Most thresholds are power density dependent (i.e., the threshold is measured in W/cm^2).

The noise equivalent power density (power density that produces a signal equal to the average noise) in a microwave receiver can be estimated from

$$NEPD = 4\,k\,T\,B\,F\,L\,/\,\pi D^2$$

where T is the electronics temperature, B is the electronics bandwidth, F is the amplifier noise figure, L is the total internal transmission line loss, and D is the diameter of the receiver antenna. Typical values of $NEPD$ range from 10^{-10} to 10^{-16} W/cm^2. A jamming signal I that is 10^3 to 10^4 times $NEPD$ will almost always overwhelm desired signals in a receiver. Thus power densities of 10^{-6} to 10^{-12} W/cm^2 can cause interference with device function. This interference will disappear as soon as the jamming signal is removed. Jamming signals 10^4 to 10^8 times *NEPD* may cause saturation in the amplifier circuits. Recovery from saturation takes microseconds to milliseconds after the jamming signal is removed.

Electronic component damage due to breakdown will almost certainly occur when voltages of the order of ten times the rated voltage are applied to them. In modern systems the rated voltages range from 3 to 15 volts. Many straight-line wire lengths between components will be between 1 mm to 1 cm in length. An imposed electric field of the order of 3000 to 150,000 V/m will therefore be required to produce the 30 to 150 V needed to cause breakdown. The rms electric field (in V/m) of an electromagnetic wave is related to the power density (in W/cm^2) by the relation

$$E_{rms} = 1942\ (PD)^{1/2}.$$

Thus, damaging field strengths can be produced by power densities greater than a threshold that lies somewhere between 2.4 W/cm^2 and 6000 W/cm^2. The wide range accommodates almost all single-lead, single-component situations. In even the simplest military electronics system, there will be hundreds of leads and components of varying lengths, sensitivities, and operating voltages, but only one needs to burn out for the hardware to fail. Thus, we may expect that a value in the range of 2.4 to 60 W/cm^2 would be sufficient to cause burnout in almost any system (with higher voltage systems being at the upper end of the range and lower voltage systems at the lower end). This is valid for unshielded components. In well-shielded systems, external field strengths will of necessity be much higher, perhaps as large as 1000 to 10,000 W/cm^2 or even larger.

Much lower voltages induced on component leads can produce digital device upset. This occurs when “0” levels are mistakenly read as “1” levels and vice versa. This will occur almost every time if the induced lead voltages are comparable to the operating voltages. In a 5 V integrated circuit, the “1” level might be specified as 3-6 V input to a device and the “0” level as 0-2 V input. If the electromagnetic field-induced voltages exceed 3 V, then if it opposes a normal 5 V signal, a “1” can be lowered to a “0”. If the induced voltage adds to a 0 V signal, then a “0” can be converted to a “1”. In practice because of the electrical noise that is always present in any electronic system and because many independent logic circuits are present in any practical device, induced voltages of the order of 10% of the operating voltage have a high probability of producing an upset. Using the same values as the preceding paragraph, we estimate that logic elements can be upset by power density between 240 μW/cm^2 and 0.6 W/cm^2. A nominal threshold for device upset can be assumed to be in the range of 0.24 to 6 mW/cm^2 for unshielded systems and 0.1 to 1 W/cm^2 for shielded systems.

Jamming of the human visual system can be accomplished by a non-injurious phenomenon known as veiling glare. Veiling glare is caused by scattering from the optical components of the imaging system – in this case the lens and vitreous humor. A detailed description of veiling glare can be found in the book by Sliney and Wolbarsht [165]. The power density needed to produce veiling glare is a function of ambient light level and wavelength. In bright sunlight, power densities in the range of 0.1 to 10 mW/cm^2 are needed. At night, power densities as low as 0.1 to 10 nW/cm^2 will suffice. By analogy, we might argue that a television-based imaging system would be no more difficult to jam with veiling glare than the eye. In fact, because TV systems typically have many more optical elements than the eye, veiling glare is often even easier to produce in TV systems than in the eye. If we take into account that TV imagers have large telescopes for image formation (and can therefore collect more jamming light), we can estimate that the power density required for producing veiling glare in a TV imager is related to the power density for producing veiling glare in the eye by the relation

$$PD_{TV} = \eta \, (d/D)^2 \, PD_{EYE}$$

where η is an optical quality factor of the TV optics relative to the eye (lacking specific data we will assume this to have a value of 1), D is the diameter of the telescope, and d is the diameter of the pupil. For daylight imaging, d = 3 mm, D = 10 cm, and PD_{EYE} = 1 mW/cm^2 yields $PD_{TV} \cong 10^{-6}$ W/cm^2, a very modest and easily achieved value. Note: a pocket laser pointer can produce veiling glare at hundreds of meters if pointed at someone's eyes (but don't try this at home without professional supervision).

Physical damage to a structural material requires the deposition of enough electromagnetic energy to heat the material to melting (or at a minimum until it softens enough to fail under applied stresses. An estimate of the energy density required to raise a material to its melting temperature can be obtained from

$$ED = \{C_p \, (T_{MELT} - T_{AMBIENT}) + \Delta H_{FUSION}\} \, \rho \, h$$

where C_p is the specific heat of the material, ΔH_{FUSION} is the heat of fusion of the material, ρ is the material density, and h is the material thickness. This estimate ignores the temperature dependence of heat capacity (which usually increases slowly with increasing temperature) and thermal conduction away from the heated region. For a 1-mm thick sheet of aluminum, ρ = 2.7 g/cm^3, T_{MELT} = 932 K, C_p = 0.9 J/g-K, and ΔH_{FUSION} = 387 J/g. Thus if the ambient temperature is 300 K, ED = 258 J/cm^2. If we assume that the energy is deposited in one second (the maximum amount of time a practical, high rate of fire weapon could spend on each target) and that the metallic surface reflects 99% of the energy, then the damage criterion becomes an incident power density of roughly 26 kW/cm^2. The value of 99% chosen for reflectance is that of a polished metal surface at room temperature. Any significant surface roughness, oxide layer formation, or coating would likely reduce this number. At higher temperatures, oxidation is almost certain to occur reducing the reflectance. In addition, many materials soften (lose their strength) at temperatures well below the melting temperature. If the material is subjected to any aerodynamic or structural loads, it will fail before melting. Thus, our calculated value is almost certainly an overestimate of the power density needed to destroy a target with a 1-mm aluminum skin. If we perform the same estimate for a 1-mm titanium sheet (ρ = 4.5 g/cm^3, T_{MELT} = 1660 K, C_p = 0.528 J/g-K, and ΔH_{FUSION} = 435 J/g) we find a requirement for ED = 520 J/cm^2, or assuming 99% reflectance, a damage threshold of 52 kW/cm^2. This probably represents the top end of the range of power densities required for structural failure. Taking all of our assumptions into account, power levels of 10 kW/cm^2 sustained for 1 second will almost certainly suffice for killing missile targets.

APPENDIX J. INFORMATION WARFARE

Information warfare is any form of warfare that directly involves the generation, processing, or transmission of information. As shown in Table J-1, there are perhaps six major elements of information warfare: command & control warfare, intelligence warfare, electronic warfare, psychological operations, information economic warfare, and cyberwarfare. The characterization shown in the table is an amalgamation of the ideas of several authors and is by no means universally accepted.

Table J-1. Scope of information warfare.

INFORMATION WARFARE ELEMENTS	INFORMATION WARFARE OPERATIONS
COMMAND & CONTROL WARFARE	ANTI-HEAD (Attacks on communications centers) ANTI-NECK (Attacks on communications links) C^2 ELECTRONIC ATTACK C^2 ELECTRONIC PROTECTION
INTELLIGENCE (or KNOWLEDGE) WARFARE	OFFENSIVE (Sensor use to determine threat character) DEFENSIVE (Counter-intelligence and Deception) SIGNALS INTELLIGENCE CRYPTOGRAPHY
ELECTRONIC WARFARE (ANTI-SENSOR)	ELECTRONIC ATTACK ELECTRONIC PROTECTION ELECTRONIC SUPPORT MEASURES
PSYCHOLOGICAL OPERATIONS	OPERATIONS AGAINST NATIONAL WILL OPERATIONS AGAINST COMMANDERS OPERATIONS AGAINST TROOPS CULTURAL CONFLICT
INFORMATION ECONOMIC WARFARE	INFORMATION BLOCKADE INFORMATION IMPERIALISM
CYBERWARFARE	COMPUTER DISEASES HACKER WARFARE INFORMATION TERRORISM SEMANTIC ATTACK SIMULA WARFARE GIBSON WARFARE

Command & control warfare (C^2W) is warfare that addresses the physical ability of commanders to receive direction from higher command, make decisions, communicate those decisions to subordinates, and receive situation reports from subordinates. C^2W can involve physical attack or electronic attack. Physical attack can involve bombs or missiles with deep penetrating warheads or submunition (bomblet) payloads or attack by ground forces. **Anti-head** C^2 attacks are designed to destroy enemy command & control centers. **Anti-neck** C^2 attacks are designed to destroy enemy communication links or communications nodes. Obviously, physical attacks require friendly force access to enemy communications nodes or command centers. In an environment in which the enemy possesses an access denial capability, physical attacks as an information warfare strategy become problematic.

C^2 electronic attack involves the use of communications jammers to degrade or deny the ability to use his electronic communication links to exercise command & control. Electronic attack is a relatively short-range capability. Depending on the system being jammed, the jammer may be as distant as a few hundred kilometers, but more often the jammers must be within a few tens of kilometers. Thus, electronic attack is also problematic in an access denial scenario. **C^2 electronic protection** involves techniques designed to preserve and protect friendly communication links against enemy electronic attack. Both C^2 electronic attack and protection used to be considered part of the field of electronic warfare.

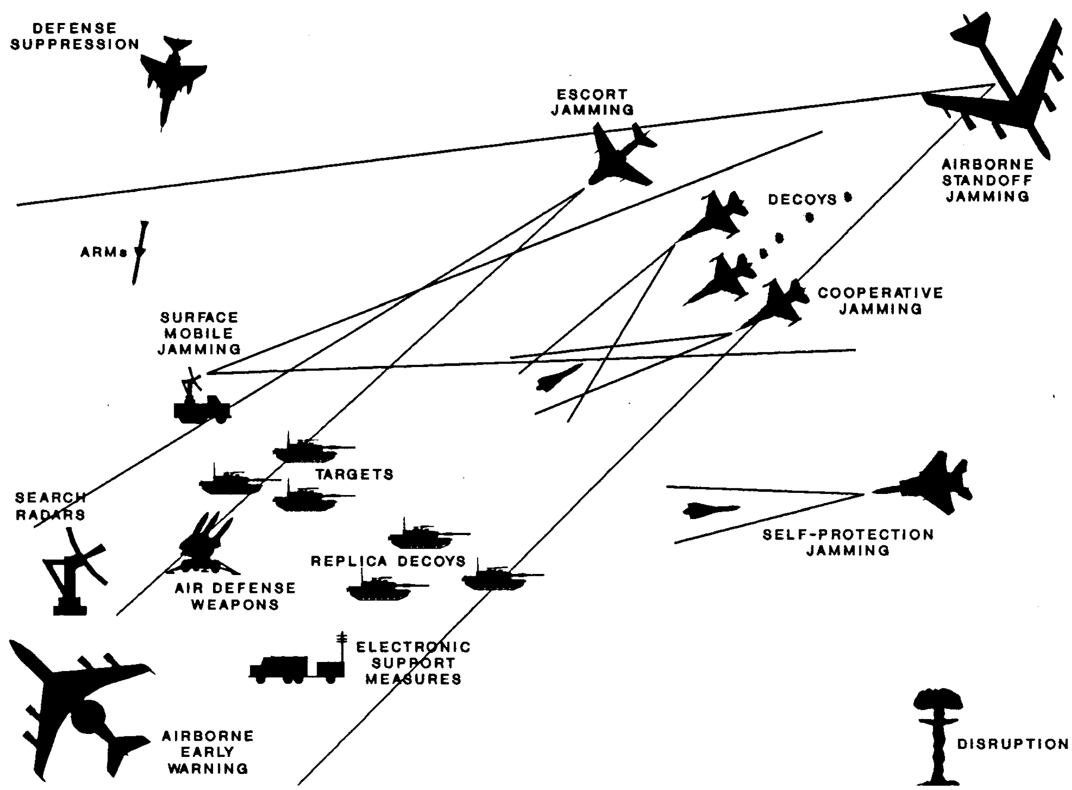
Intelligence warfare (or knowledge warfare – KW) involves actions designed to determine the composition, disposition, and intent of the threat. **Offensive KW** operations involve the employment of sensors to characterize the threat. These sensors may be on satellites, unmanned vehicles (air, ground, or submarine), or manned platforms (aircraft, submarines, surface ships, or ground vehicles), or deployed from such platforms. Specific operations involve deployment of the sensors, acquisition of intelligence data, transmission of intelligence data, and possibly recovery of the sensors. Forces in the field might be involved in launching, flying, and recovering unmanned air vehicles (UAVs) carrying radar, passive microwave, infrared, or television reconnaissance sensors. They might carry high-resolution night vision sensors to the front lines to spy out enemy positions. They might use patrol boats to deploy small acoustic detector networks in littoral waters to track diesel submarines. As with a number of other forms of information warfare, if an adversary possesses an access denial capability, offensive knowledge warfare operations may be difficult or impossible to perform.

Defensive KW operations involve the denial of these sensor-based intelligence capabilities to the enemy. These may involve anti-sensor operations (electronic warfare or physical attack), denial of access to critical areas to enemy sensor platforms, and strategic deception (presentation of misleading information to the enemy's sensors). Development of weapons to specifically target and destroy UAVs would facilitate an important class of defensive knowledge warfare applications. Antisatellite operations also fit under the umbrella of defensive KW.

Intelligence warfare also includes **signals intelligence** and its relative **cryptography**. Signals intelligence involves the collection of radar, radio, and other electronic transmissions made by the enemy and their processing, understanding, and exploitation. In many instances the signals will be encrypted, in which case, cryptography, the art of decrypting encrypted signals, plays a significant role.

<u>Electronic warfare</u> has a somewhat reduced status in the new hierarchy of electronic threats and capabilities. Today it is almost exclusively aimed at sensor (e.g., radar) performance. Nevertheless, it is still a complex subject, as illustrated by Figure J-1. Radars and radar-guided missiles are located everywhere. Jammers abound on platforms of all kind. Both sides may employ dedicated standoff jammers (usually denial jammers as described below). Air strikes may be accompanied by escort aircraft carrying a variety of denial and deception jammers. Aircraft will be provided with self-protection jammers (usually deception type) and decoys. Flights of aircraft may use their self-protection jammers in cooperative fashion to enhance their effectiveness. Radars and jammers may be targeted by anti-radiation missiles. Lastly, directed energy weapons and nuclear EMP will add the potential for catastrophic destruction of both inadequately-designed radars and jammers.

Figure J-1. The electronic warfare environment.



Electronic attack involves those operations designed to degrade or deny the enemy the use of the electromagnetic (and/or acoustic) spectrum. There are acoustic analogs (useful against sonar systems) to almost every electromagnetic electronic attack technique (useful against radar systems). **Denial jamming** seeks to introduce sufficient noise into a sensor system such that desired signals cannot be reliably detected or analyzed. Key denial jamming techniques include barrage noise (broadband noise radiated throughout a specific waveband), spot noise (narrowband noise radiated at a single frequency), rail jamming (transmission of very short pulse trains at very high pulse repetition frequencies), and bright light sources (for jamming optical and infrared sensors).

Deception jamming seeks to introduce signals into a sensor system that the sensor system will mistake for the desired signals and initiate incorrect actions. Significant deception jamming techniques include the following. Inverse gain is a technique used against conical scan radars in which the received signal is retransmitted with a gain that is inversely proportional to the received signal strength. Range gate walkoff is used against range-gated radar trackers and involves retransmitting the amplified received signal with successively longer (or shorter) delays. The strong signal captures the radar and walks the system off the true target range by the changing delays, until the true range is outside the radar's range gate. When the jammer is turned off, the radar can no longer detect the true target return. Velocity gate walkoff and automatic gain control capture (AGC) work in roughly similar fashion. In velocity gate walkoff the frequency of the retransmitted signal is gradually shifted until the target's Doppler shift is outside the velocity gate of the radar. In AGC capture, the amplitude of the retransmitted signal is gradually increased causing the radar AGC to gradually turn the gain to minimum. When the jammers are turned off, the true target signals are no longer detectable. Delta jamming transmits strong signals at two frequencies. In the radar receiver the signals essentially act as local oscillators for each other. The frequency difference of the two transmissions is varied in a fashion to produce whatever frequency waveform the radar is expecting but bears no relation to the signal the target return would have produced. Cross-eye jamming involves transmitting the same signal from two separated antennas with a half-wave phase shift between them. In a monopulse receiver, the two signals will produce an output that appears to come from a slightly different angular position from the real target position. Crosspole jamming involves transmitting the same signal from two separated antennas with different polarizations. This too tends to cause monopulse receivers to have angular errors. In addition to those mentioned above, there are hundreds of specific denial and deception jamming techniques, a few of which that can be made to work against almost any kind of sensor system. They exploit almost every conceivable weakness in sensors' signal reception and processing systems.

Decoys are physical deception devices that attempt to mimic the target characteristics that an enemy system is attempting to exploit. The aim is to get the enemy system to accept the decoy as the real target and subsequently ignore the real target. Chaff is a cloud of thin metal strips or fine metal wires that when dispersed in the atmosphere will produce a large radar cross section (RCS). The chaff radar cross section must be significantly larger than the target radar cross section for chaff to be effective. Each piece of chaff produces a specific average cross section. Thus larger RCS targets require more chaff to act as effective decoys. Retroreflectors (corner reflectors) are also used as radar decoys. In addition to having a large RCS, active expendables emit radio frequency radiation that matches the target emission to fool electronic support measures systems. Flares are used as decoys against infrared sensors. To be effective the flare must emit more infrared radiation in the sensor waveband than the target emits. The total emission is proportional to the area of the emitter and the Planck spectrum (see Appendix H). Since flares are much smaller than the target they must be much hotter to allow the Planck function to outweigh the smaller area. Flares can be made with shrouds to alter the color characteristics of the emissions. They can be fitted with aerodynamic bodies to better simulate the motional characteristic of an aircraft target. Flares and chaff can be combined using pyrophoric metals to yield "hot chaff". Decoys for ground systems can involve balloons with the shape and color of desired targets (and possibly augmented to have desirable RCS and infrared emission as well as shape and color). Silhouettes are easy to make and surprisingly effective. Shells which replicate the shape of vehicles can be fitted to automobiles or jeeps to simulate much larger and more important armored vehicles. Even shadows on the ground can be simulated to hint at the existence of targets that don't exist in reality. The science of electronic warfare is quite advanced and exceedingly creative. Many other decoy variations exist beyond those mentioned here.

Electronic protection involves those actions taken to protect friendly use of the electromagnetic (and/or acoustic) spectrum. Sensors can be hardened against overload from intense electromagnetic signals. Electronic counter-countermeasures are techniques designed to complicate radar waveforms and processing to levels that are difficult for deception jammers to duplicate. The use of spread spectrum waveforms is one of these techniques. Jamming at a single frequency will have its effectiveness reduced by the ratio of the jammer bandwidth to the spread spectrum bandwidth. Rapid frequency jumping is another electronic protection technique. In general, electronic protection measures are implemented to overcome whatever specific electronic attack techniques are brought to bear against it.

Electronic support measures includes action taken to exploit the enemy's use of the electromagnetic (and/or acoustic) spectrum. It includes interception of enemy sensor emissions, identification of the source(s) of those emissions, and the location or localization of the source(s) of those emission. Modern interferometer arrays can localize emitter direction to less than a radar beamwidth. They can detect virtually all amplitude and frequency modulations characteristic of a given emitter, thus permitting the emitter identification. This permits consideration of attacks (possibly using anti-radiation missiles) against those emitters.

Psychological operations are those operations aimed at affecting the enemy's mental toughness, his desire to continue to fight, and his mental ability to fight effectively. **Operations against the enemy's national will** are designed to instill questions in the minds of the enemy's people and civilian leadership. Such questions include:

Can we win the current (or impending) conflict?
What do we have to sacrifice in order to win?
How will I (or my family) personally fare if we continue to fight and lose?
What happens to our way of life if we continue to fight and lose?
Is the expected sacrifice worth the potential payoff if we win?
Can I trust my government and its leaders to do the right thing for the country?
Are we fighting for an acceptable reason?

One type of national will operation conducted in advance of open conflict uses a technique that can be described as the velvet glove ("Accept us as friendly") covering the iron fist ("or else"). That is, if the adversary goes along with the desired policies, then benefits will flow. If it opposes those policies, then retribution will follow. Propaganda in the media (foreign and domestic), leaflets, and radio and television broadcasts, as well as government to government communications are among the physical tools employed.

Operations against the enemy's commanders are designed to confuse or disorient the operational commanders. Such operations may suggest that their subordinates are disloyal, or that their superiors are planning to betray or sacrifice them. They may play on perceived predisposition of a commander. For example, the Allies in WW II perceived that the German forces, and especially Adolf Hitler, were convinced the invasion would occur at the Pas de Calais. Deception plans successfully exploited this perceived predisposition by reinforcing it. Some operations might aim to enrage an unstable commander. If he can be made sufficiently angry he will lose his objectivity and change his operational mode from proactive to reactive. For example, "accidental" capture of a home video showing an adversary unit performing a skit in which the unstable commander is portrayed as a laughingstock or as an incorrigible pervert is likely to unhinge that commander when he views it. This is even truer if he knows his subordinates have had the opportunity to make copies of the video.

Operations against troops are designed to disaffect the direct fighting forces. They may attempt to instill fear of death or injury. They may be designed to instill fear for the safety of family or friends. They may attempt to build on the natural resentment between those serving in the trenches and those staying on the "home front". Messages, pamphlets, magazines, or movies showing images of "4-F" types seducing the wives and girlfriends of soldiers doing the fighting exacerbates the effects of the real "Dear John" letters that will be received by any sizable collection of people undergoing enforced separation. Having a "daisy cutter" bomb or a B-52 raid strike the regiment next to yours, followed immediately by being bombed by leaflets explaining that your regiment's turn will come tomorrow at 0900 is guaranteed to instill fear in any soldier and make him consider going over to the other side. News broadcasts showing natural disasters and mass murders back home will cause soldiers to be concerned for their families, especially if mail call or telephone access has not been forthcoming.

Cultural conflict involves the perceived disruption or corruption of fundamental beliefs and values. It is a common source of conflict and internal unrest. Western European culture is often in conflict with Middle Eastern and Asian cultures. In countries whose governments have made attempts at "westernization", the oldest generation begrudges the changes they are forced to make and mourns the loss of the old ways. The youngest generation (finding something lacking in their lives) demands the return of the abandoned traditions that they identify as the reason for their feelings of loss. The two generations often unite against the middle generations (who often wield the economic and political power) to demand reversal of the changes. Sometimes this can become open revolt. At other times the unrest is directed at the most visible representatives of the West. Once a multicultural conflict has been engaged, the cultural differences facilitate the demonization of the enemy, making it easier on the conscience to kill them.

As an offensive tool, cultural conflict might be exploited in operations designed to convince one opponent that its current allies are attempting to corrupt its way of life. This is a frequent claim by Iran made in an attempt to weaken the alliance of other Persian Gulf states with the United States. When backed up by believable evidence, the technique can be effective. In 1857, British troops in India (regular and native) used the Minie cartridge. This greased paper cartridge had to be bitten before loading. Disaffected native troops spread the word throughout the ranks that the cartridges were greased with fat from pigs (unclean to Moslems) and cows (sacred to Hindus). When 85 sepoys were punished for refusing to use the cartridges, the general unrest turned into the Great Mutiny of 1857-1858. Later investigation showed that some of the cartridges were indeed greased with pig or cow fat. [166] Regardless of the truth of the "rumor", this is an excellent example of an information operation involving cultural conflict.

Information economic warfare is economic warfare that takes advantage of the distinct economic value of information or access to information. For example, access to the Internet is a sign of a modern organization or individual. Yet Internet access is not a right; it must be negotiated with the operators. Access can be denied and it can be revoked after it has been granted. **Information blockade** is the interdiction of existing vital information flows to an adversary until desired concessions have been obtained. Access to the Internet might be physically interdicted. The use of electronic international banking or securities exchange can be severed. Access to satellite imagery used in natural resource management can be denied (as access to SPOT imagery was withheld from Iraq during the Gulf War. These actions can cripple an economy or permit a poor economy from having any of the benefits of the world economy and its growth.

Information imperialism involves preferential offering of access to valuable or desirable information in exchange for support or concessions. Imagery from intelligence satellites is a highly desirable commodity. Any selective sharing of such data is sure to warrant a steep price from the receiver. Even earth resources satellite images can be worth a fortune to a country looking to develop and exploit its mineral wealth. Information can also include the data needed to exploit new technologies. A computer code that can integrate national weather measurements and generate accurate forecasts has significant value. Computer-aided design and computer-aided manufacturing software is data with major economic value. Seismic sounding data might show structures with a high probability of containing oil, gas, or pure water. Only a few countries around the world can generate the data described above. Those countries control the access to that data for both economic and political reasons.

Cyberwarfare is the branch of information warfare that actually involves computer operations. **Computer diseases** include computer viruses, worms, Trojan horses, and other nasties. They are typically attached to software that is exchanged between computers. Once the software is received by a computer, the disease activates itself, makes replicas of itself and attaches them to other software that is destined to be transmitted to yet other computers. The disease may or may not affect the host machine in a malicious way. It may simply display a message on a monitor. It might command the host computer to erase certain files. It might command the host computer to format its disk drives, causing total data loss. The disease may contain an operational trigger (activate when program XYZ is run) or a time-based trigger (activate on a certain date) for these actions. Sometimes the diseases have little direct effect on the computer but have a serious cumulative effect. For example, a disease may create ten (or some other number of) copies with random names every time it is triggered. Over time, more and more copies accumulate in memory until the memory is entirely consumed. The Internet Worm made and transmitted exponentially more copies of itself as time progressed until the transmission medium became saturated and real messages could no longer be transmitted. The net was forced to shut down. Otherwise, it was designed to be totally benign. Diseases can be transmitted in executable files, in electronic mail attachments, in macros appended to word processing files, and in many other ways. Many people think of computer viruses first when they think of cyberwarfare.

Hacker warfare is another form of information warfare that many people commonly envision. Hackers (perhaps better called cyberwarriors when professionals are involved) gain access to individual computer systems and modify the host software in such a fashion to:

* Deny one or more functions of the computer system to the user.
* Destroy stored data.
* Alter stored data in a covert fashion .
* Acquire and transfer stored data in a covert fashion (computer espionage).

The tools hackers use to gain access are freely shared on the web and computer bulletin boards. A single hacker can cause major damage to a number of computer systems. If that damage were multiplied by tens of thousands if a full corps of cyberwarriors were established by an adversary, the results might be beyond comprehension.

Information terrorism is related to hacker warfare (it must either use hackers or insider help) but involves the disruption of civilian and/or military affairs through an attack or possibly multiple attacks on critical computer-controlled systems. The aim is not the denial of the computer function, but denial of the function of the system controlled by the computer. Shutting down the air traffic control system in a region, with the subsequent probability of airliner crashes and the certain slowdown in air travel is a prime example. Attacks may be preemptive or unannounced. They may be announced in advance (essentially holding the system as hostage). Included among the kinds of things of which information terrorism is capable are:

* Disrupting electrical power service to large regions of the country,
* Invalidating the transactions of the major stock exchanges,
* Performing major untraceable transfers of funds between all of the accounts of a number of major banks,
* Shutting down the control signal and switching system of the national railroads,
* Trapping trains in the middle of subway or undersea tunnels, and
* Creating massive traffic jams by shutting down the computers that control traffic lights in a major city.

Semantic attack involves the alteration of host computer programs in such a subtle way that erroneous output is generated even though the system is perceived to be functioning normally and the erroneous output is accepted as error-free. Obviously a hacker or insider help is needed to perpetrate a semantic attack. A semantic attack on a national air defense system might convince an adversary that it was under attack. The reaction to this conviction in the form of an "unprovoked attack" on friendly assets could cost the adversary the benefit of world opinion and justify a massive (and pre-planned) retaliation by friendly forces. Semantic attack might cause the insertion of false targets or forces into the situational awareness picture of a commander. In an air defense weapon's computer system it might cause subtle guidance errors in command-guided missile systems causing them to miss their targets. In a logistics computer system it might cause less materiel than requested to be shipped to the proper destination or it might cause all of a critical component to be shipped to a single site with no use for the part. The effects of semantic attack can be devastating to a military force (or for that matter, a commercial or governmental entity). Obviously semantic attack requires detailed knowledge of the system being attacked and its associated software.

Simula-warfare is warfare waged by mutually simulated battles rather than through real battles. This is the computer equivalent of battle between heroes (such as David vs. Goliath). The watch phrase is "my computer simulated force is better than your computer simulated force". Simula-warfare is possible today. On the one hand, it is unlikely that hostile parties would abide by the results. On the other hand, the outcome of a truly realistic simulation might convince one party that it is likely to lose a real confrontation and therefore be more amenable to negotiation of a settlement. It might also convince the other party that it would easily win the real confrontation and make the conflict inevitable. One-sided simulations are routinely used by the major powers to plan and evaluate their forces.

Gibson warfare is a potential form of future conflict in which virtual creations wage real war in cyberspace with real consequences. This is currently only science fiction. However, in the reasonably near future we may have near global, wireless access to the Internet. Direct neural connection between humans and computers is also soon to be developed. When everyone's brain is directly connected twenty-four hours a day to a global Internet, the conditions for Gibson warfare will have been established.

APPENDIX K. NONLETHAL WEAPONS

Nonlethal weapons (NLW) are devices or chemical agents whose primary purpose is other than inflicting lethal injury on an adversary. They may be intended to disable or incapacitate personnel, they may be intended to disable or incapacitate equipment or vehicles, or they may be intended to destroy equipment or vehicles that do not have human occupants or operators. Many NLW do possess the potential for lethal effects against humans. Because of this, NLW are sometimes called less-than-lethal weapons.

Non-nuclear electromagnetic pulse (EMP) weapons, high-power microwave (HPM) weapons used against electronic systems, and information weapons (computer viruses or other pathogenic software such as Trojan Horses, worms, or logic bombs) are often classified as NLW. Nuclear EMP is discussed in Appendix A. Non-nuclear EMP and HPM weapons are discussed in Appendix I. They will not be discussed further. Information warfare and information weapons are discussed separately Appendix J.

Good NLW have several requirements that they should meet. They should contribute to the accomplishment of a task or tasks that may be assigned to military or law enforcement forces. They should be consistent with established policies including laws, treaties, arms control agreements, or other legal obligations the government is committed to observe. They should be technologically and operationally feasible. They should have an acceptably low probability of being fatal or inflicting permanent disablement on personnel, and causing undesired damage to property and the environment. They should not be capable of being easily defeated by enemy countermeasures once their operational principles are known; or if they could, the benefits of a single opportunity to use them in a given context should be so great as to outweigh that disadvantage. In the paragraphs below we describe a number of different candidate classes of NLW.

Non-penetrating projectiles include bullets, pellets, or ring airfoils that will not penetrate the skin but will deliver significant kinetic energy and momentum to the target. The projectiles will produce significant pain similar to a punch with a fist or a knuckle. The intent is to produce a noticeable and highly unpleasant, yet minimally damaging impact. Larger projectiles may be used to knock an individual off balance. Projectiles may be made of rubber, wet sponges, beanbags, or compressed powder (like chalk). They may be fired from rifles, shotguns, or grenades. Obviously, the projectiles can cause serious injuries if they strike the eyes or gonads. Individuals reacting to the impacts may subject themselves to indirect injuries from falls.

Flash-bang devices are pyrotechnic devices (usually grenades) that produce intense sound (200 dB at 1 meter distance), high pressure waves, and blindingly intense light. The combined sound, pressure, and light saturate the human sensory system. Any individual within a few meters of a flash-bang explosion is stunned (unable to process any sensory input or command motor responses) for periods up to six to eight seconds. The device is designed not to produce any fragments or ballistic motion. There is some possibility of hearing and/or vision damage if the device explodes too close to an individual's head.

Lacrimators are chemical agents that irritate the mucous membranes and produce intense tear production, eye pain and throat congestion. They are commonly called tear gases, even though they are seldom dispersed as gases. Common examples are the chemical agents CN (Mace), CR, CS, and OC (Pepper Oil). **Sternutators** are chemical agents that irritate the respiratory passages. They produce violent sneezing, ultimately inducing severe nausea and vomiting. As a result they are commonly called vomiting or nausea agents. Common examples are the chemical warfare agents DA, DC, and DM (Adamsite). Lacrimators and sternutators have been commonly used in riot control. They are commonly dispensed from pyrotechnic grenades, although they can be dispensed on large scales from aerial spray tanks. They are very effective at incapacitating unprotected individuals. Complete recovery occurs within a few minutes to an hour, once exposure to the agent is terminated. The high toxicity of the sternutators has caused them to be removed from service by most countries. For the same reason CN is now seldom used in the United States. Deaths have occurred from the use of any of these chemicals, even OC, although they are rare with CS and OC.

Electric stunners produce high voltage shocks in the targeted individuals. The shock is sufficient in amperage to cause muscular inhibition, but not ventricular fibrillation or death. Stunners include tasers (guns which shoot twin barb-ended wires connected to a capacitive pulse forming system), cattle prods (batons with two closely spaced electrodes at one end connected to a pulse forming system), electrically charged fences (these can be designed to be lethal, stunning, or merely "shocking"), and electrically charged objects (commonly door handles).

Water cannons use high-pressure water streams to knock targeted individuals off their feet. The simplest implementation is fire hoses, although specialized pump and nozzle systems (such as those found on fireboats or some fire engines) can be used with greater accuracy at longer distances. Obviously if the water cannon can knock someone off their feet, the resulting fall may be capable of producing injuries.

Vortex ring projectors are devices that create and direct vortex rings against distant desired targets. Vortex rings are donut-shaped volumes of air that rotate about the azimuthal axis of the donut. The azimuthal axis is oriented perpendicular to the ring's direction of motion. Molecules of air are trapped within the vortex and will propagate with it. Vortex rings can maintain their shape and character for many seconds to minutes after formation and can propagate distances of hundreds of meters. The primary function of a vortex projector is to deliver a pulse of energy and momentum to the target. A vortex ring can knock an individual off his feet. It can hypothetically knock an aircraft out of the air. Note that wake vortices from large jetliners have been known to cause small aircraft to crash. Vortex rings can also be used to carry chemicals or small particles with them. Thus a vortex ring projector might be used to deliver a puff of tear gas, calmative agent, or malodorant (see below) to a specific target from long distance. It might also be used to deliver lethal chemical or biological agents to specific targets.

Tranquilizer dart guns are commonly used by zoologists and animal control personnel to sedate dangerous wild animals so that they can be safely transported. There is nothing physical to prevent their use on humans. There is always danger of adverse reactions and damage induced by having the hypodermic dart strike bone a bone or the eye. It is possible that future improvements might eliminate the hypodermic dart, replacing it with small, highly soluble projectiles (needles) that would penetrate the skin, rapidly dissolve (or melt), and thereby release the tranquilizing agent.

Infrasound projectors are devices that create sound with frequencies below the range of human hearing (nominally <20 Hz) and direct it against desired targets. Infrasound resonates with the internal organs of the body to produce rapid discomfort, nausea, and loss of bowel and bladder control. Complete recovery takes many seconds to minutes. At high enough levels, it may resonate with other material structures, causing them to undergo amplified vibration followed by possible structural failure. A large infrasound projector could induce the equivalent of an earthquake in a structure causing walls to fail and the building to collapse. Modern infrasound generators consist of small open-ended combustion chambers that are alternately filled with fuel-air mix and ignited at rates of a few Hz. Tubes or parabolic reflectors can serve to direct and concentrate the radiation at an intended target.

Sensor aperture coatings are opaque adhesive materials applied to the external apertures (windows or domes) of sensors. The materials coat the apertures and block signals entering or leaving the apertures. A multitude of materials could be employed. A thin layer of mud on the window of an electro-optical sensor will destroy its performance. Unfortunately, many sensor systems have window washers to counter this occurrence. Paint is a better choice. It can be delivered in spray form and has adhesive properties that make it difficult to remove. Heavy oils and petrolatum can also be used. Metallic paints (powdered metals in adhesives or heavy oils) can be used to coat radomes negating the performance of the radars that those radomes are supposed to protect.

Obscurants and smokes degrade the ability of many sensor systems to provide visual information about targets and their movements. Smoke may be used to hide actions that might appear provocative to assembled crowds or adversaries. Smoke may be used to protect troop movements and delay directed fire until separation decreases to hand-to-hand combat ranges. Although not exactly weapons, the cost-effective protective action of smokes and obscurants, with almost no collateral or long-lasting effects, warrants their inclusion.

Laser dazzling weapons are intended to temporarily blind humans and electro-optical sensor systems. Temporary blinding of humans can be accomplished by flashblinding or veiling glare. Flashbinding is an effect in which the visual receptors are saturated. An afterimage results whose intensity decays slowly with time. As long as the afterimage brightness exceeds ambient light levels, the exposed individual cannot distinguish objects in his environment (he sees the afterimage, not the real image). Flashblindness can last from second to many minutes, depending on ambient light levels. Veiling glare is produced by scattering in the eye. The scattered laser light produces a strong illumination over much of the retina. When this scattered illumination exceed ambient illumination levels, the real images are veiled by the scattered light. The effects of veiling glare disappear as soon as the laser beam illumination is removed. Both flashblindness and veiling glare can be produced by laser intensities below those levels at which eye damage can occur. Nevertheless, a device that can flashblind an individual at 100 meters may be capable of permanently blinding an individual at 10 meters. There is an attempt to produce an international accord that bans laser-blinding weapons. The U. S. is not a signatory to this accord. Laser dazzling weapons would technically be allowable under the proposed accord, although any use at ranges where blinding was known to result would be illegal. The potential confusion and inadvertant violations that might result has resulted in U. S. policy that we will not develop or deploy such devices.

Isotropic radiators are pyrotechnic light sources. Explosive shock waves propagating through inert gases produce blackbody temperatures at the shock fronts of tens of thousands of degrees Kelvin. Blackbody radiation from these shockwave light sources is much brighter than the sun. A single artillery-delivered isotropic radiator could be used to flashblind all unprotected individuals within hundreds of meters of the explosion. With one side wearing protective eyewear, use of isotropic radiators at the outset of a direct assault could temporarily blind everyone on the opposing side at the critical moments when they need their vision the most.

Bucha strobes are colored lights (typically red or blue) that flash at frequencies near the frequency of brain waves. Their effect is to alter brain function similar to that in petit mal epileptic seizures. Within seconds, affected individuals would rapidly become disoriented and probably nauseous. There is concern that a fraction of the population may not be affected by such strobes.

Microwave projectors can be used as anti-personnel weapons as well as anti-materiel weapons. Appendix I discusses the use of high-power microwaves (HPM) against electronic systems. The potential for anti-personnel applications warrants discussion in this appendix as well. Depending on the frequency, intensity, duration, and waveform projected, microwaves can cause a variety of effects in humans and animals. They can cause either readily noticeable or very subtle overheating and fevers. They can induce memory impairment. They can cause complete temporary neural overload (stunning), pseudo-epileptic seizures, and even cardiac arrest. Radar transmitters have also been known to produce detectable sounds in the human ear. It is theoretically possible that a properly modulated microwave projector could create intelligible speech in an irradiated target's ears. The possibilities of this in psychological warfare might prove most interesting.

Conductive strand chaff consists of long strands of carbon fiber or long thin metal strips or long metal wires. When dispersed over an area, the chaff will drift into power lines or transformers shorting them out and producing power outages. It is often impossible to restore power until all of the chaff has been cleaned away from the power equipment and the nearby areas (wind can blow any uncleared chaff back into the equipment at later times).

Metal embrittlement agents are chemicals that when applied to metals will alter the molecular structure of the metal in such a fashion as to cause it to become brittle. The embrittled metals will later fail under operating stresses. For example, a metal embrittlement agent applied to supports of a bridge could cause it to collapse when a convoy of vehicles or a railroad train passed over it. Hydrogen is a common embrittlement agent. However, it is difficult to employ in tactical situations. The liquid metals, mercury and gallium, are also known to be embrittlement agents to certain structural alloys.

Supercaustics and **superacids** are bases stronger than sodium hydroxide or acids stronger than concentrated sulfuric acid. Cesium hydroxide is an example of a supercaustic. It readily dissolves glass. Methylsodium is another supercaustic. One class of super acids is based on mixtures of metal fluorides and hydrofluoric acid (for example, an equal mixture of antimony pentafluoride and hydrofluoric acid). The metal fluoride forms a complex that binds fluoride ions much more strongly than hydrofluoric acid binds fluoride ions. The result is an activation of hydrofluoric acid to an acidity orders of magnitude stronger than normal. Superacids can dissolve almost all metals and glasses. Only a few plastics such as Teflon are unaffected. Relatively small amounts sprayed on vehicles or equipment could render them unusable by etching windows and optical components or by weakening metal structures or destroying critical metal parts such as wiring.

Calmative agents are pharmaceutical chemicals that have a sedative or hypnotic effect on exposed individuals. If a riotous crowd were sprayed with such agents, their levels of emotion and motivation could be reduced to the point that they would no longer be capable of acts of violence or unrest. Such agents are likely to be considered as incapacitating chemical agents and would be banned by the intent of the Chemical Weapons Convention. The powerful narcotic fentanyl and its chemical relatives comprise one potential class of calmative agents.

Traction modification agents are chemicals or mixtures that either reduce traction by lubrication or to increase traction by adhesion. Super-lubricants can be sprayed on roads, ramps, staircases, ladders, etc., to make them impassable. Anyone attempting to use them will not be able to gain sufficient traction to exert any lateral force. Adhesives can be placed on the same surfaces to slow down and eventually immobilize moving objects (personnel or vehicles). A classic example is the tar pit (such as at the La Brea tar pits). Any animal contacting the sun-warmed tar will get stuck (permanently in the case of the tar pits).

Tire deflation devices are designed to deflate the tires of moving vehicles causing them to slow down or possibly lose control. Tire deflation devices include caltrops (small objects that look like a child's "jacks" with sharp ends) that can be scattered across a road or alleyway and erectable spike strips that can be laid completely across a road or a lane of a highway. Spikes may be hollow to permit deflation over extended time frames to minimize the potential for loss of vehicle control.

Polymer modification agents are chemicals designed to alter the physical properties of common polymers. Hypothetical examples of polymer modification agents include the following. One agent might be used to dissolve rubber in tires to disable vehicles or in gaskets to violate the hermetic integrity of a compartment. Another agent might be used to make lexan windscreens so brittle that they would shatter under mild aerodynamic stresses. Yet another agent might turn a polymer lubricant (such as Teflon) into an adhesive.

Foams are low-density materials filled with long-lasting bubbles. Sticky foam is made from resins that have strong adhesive properties and take long times to set. Once stuck to an object (such as a running adversary), it will not easily come off and one piece of foam tends to stick to another piece of foam. Spraying such foam on an adversary will quickly immobilize him. Special solvents are required to remove the foam and restore mobility. In large quantities, sticky foams can prove lethal. If a target falls and thoroughly covers his breathing passages, he will eventually suffocate. Hard foams are similar to sticky foams except that they set more quickly (seconds to minutes). This kind of foam can be used to create barriers to personnel and vehicle mobility. It can also be used to immobilize dusts or liquids (such as NBC agents) and can be used to absorb significant amounts of explosive energy. Aqueous foams are foams based on water and can be easily produced in large quantities. Unless the foam is directly inhaled or ingested in large quantities, the foam is breathable. Aqueous foam can be used to carry irritants, malodorants, or calmative agents. It can also be used to limit mobility either directly (speed through a foam is much less than without the foam) or by using it to conceal devices such as entanglement nets.

Combustion alteration agents are chemicals that change the combustion properties of fuels, making them burn more or less efficiently. The chemicals may be added to fuel supplies via sabotage or ingested along with air for combustion. An efficiency-enhancing additive, such as acetylene in air, could make an engine run considerably faster or hotter, or subject it to uncontrollable detonation (knock) that would rapidly lead to wear and engine damage. An efficiency-reducing additive would result in less energy and power per unit fuel consumption. Vehicles with such additives could not carry their intended loads or travel at maximum speeds. The ultimate in efficiency-reducing additives would halt combustion entirely, making the fuel unusable. Other efficiency-reducing additives might produce by-products that are detrimental to engine life and performance. Sugar added to gasoline will produce rapid carbon deposition that will eventually prevent proper ignition. Yet another class of additives changes the viscosity of fuels so that they are improperly fed into the combustion chambers. Wax added to gasoline, causing carburetors to clog up, is an example of such a viscosity-changing additive.

Filter-clogging agents are chemicals that can polymerize or otherwise adhere when they come in contact with the fine mesh structures of air (or possibly water) filters. Sprayed as an aerosol around a vehicle with a running engine, the ingested agent would soon completely clog the air filter causing the engine to stop. Special solvents would be required to clean the filters once clogged. There is some concern that such agents might have serious health effects if absorbed into the lungs of nearby individuals. It is conceivable the agents might act to block the smallest respiratory passages, just as they block the filter passages. Proper chemical design should be able to eliminate this possibility.

Entanglement devices are basically nets. The nets may be projected by special guns, called netcasters or netthrowers. They may be erected across roads to act as barriers. They may be dropped from elevated platforms. They may be towed by small boats or submersibles. Gun projected nets will entangle and trip up running adversaries. Barriers nets can slow down and stop moving vehicles. Similar nets are used on aircraft carriers to land aircraft that have dysfunctional arresting hooks. Marine nets can be used to foul propellers of large boats. Such nets may be made with very strong multi-strand steel cable to prevent them from breaking under the stresses produced by the ship's propulsion system.

Biological fuel-eaters are microorganisms genetically engineering to metabolize hydrocarbon fuels. It is conceptually possible to create an organism that requires only hydrocarbons and oxygen to live. Waste products would likely render the fuel unusable. Such an organism could be introduced into adversary fuel supplies to destroy them. If not detected early enough such contamination could spread to virtually every vehicle drawing from the infected supplies and possibly beyond, rendering every vehicle inoperative. Disinfection would be a tremendously costly and time-consuming process. Analogous organisms could be engineered to eat other critical materials such as plastics, rubber, plant fibers, etc. Microbial weapons of this type will almost certainly be considered to violate the Biological Weapons Convention, although they are not explicitly addressed by it.

Malodorants are chemical with extremely strong and usually offensive odors. For example, butyl mercaptan has the characteristic odor of skunk, skatole has the odor of fecal matter, cadaverine has the odor of rotten meat, and n-butyric acid has the odor of vomit. Sprayed onto individuals, a malodorant can instantly convert them into social outcasts. Others will leave their presence to avoid the smell. Malodorant attacks on leaders can disrupt the command and control of all but highly disciplined organizations. Most individuals whose bodies or clothing are partly covered with malodorants will attempt to leave the area and clean themselves up. Malodorants cannot form an impenetrable barrier, but they can discourage all but determined attempts to cross a contaminated zone. Sprayed over a large area, a malodorant will prevent casual lingering in or even transit of that area.

The list presented above is as complete as the author can make it at this time. However, it obviously cannot be all-inclusive. There are undoubtedly many other materials and devices (some of which may not yet have been invented) that have weapons applications without necessarily having lethal consequences. It should be noted that some of the classes of nonlethal weapons described above have not been reduced to practice. They remain areas of basic research. Others have been used for years as riot control measures.

Figure K-1 reprises the above list of possible nonlethal weapons. The figure also lists those characteristics that might limit the utility of each class of weapon. For example, some NLWs may violate treaties or current policies. Other NLWs may have a substantial probability of causing fatalities or long-lasting injuries. Still other NLWs may cause environmental damage or have persistent effects that are difficult to remediate. Still other NLWs have effects that cannot be limited to the intended targets, and therefore have the potential to produce collateral damage to either personnel or to equipment. For each class of NLW and utility-limiting characteristic Figure K-1 gives an estimate of the likelihood of the characteristic actually limiting the utility.

Figure K-2 lists ten common functions that have been identified for nonlethal weapons to perform:

- Incapacitate or subdue single persons
- Incapacitate or subdue large groups
- Disperse or disrupt crowds
- Assist forced entry into structures
- Disrupt personnel mobility (restrict free movement or access)
- Stop moving vehicles (fleeing suspects, vehicular assault, roadblock runners, etc.)
- Negate sensor functions
- Damage critical electronic systems (especially weapons-related or C^2-related)
- Damage critical mechanical structures (vehicles, bunkers, bridges, towers, etc.)
- Negate the electrical power system (locally or regionally)

Each of the classes of NLW has been evaluated for its utility in performing these functions.

Figure K-1. Utility-Limiting Characteristics of Nonlethal Weapons.

UTILITY-LIMITING CHARACTER → NONLETHAL TECHNOLOGY	VIOLATES TREATIES OR POLICY	MAY CAUSE FATALITIES	MAY CAUSE CHRONIC INJURIES	MAY CAUSE ENVIRONMENTAL DAMAGE	EFFECTS PERSIST; REMEDIATION DIFFICULT	COLLATERAL DAMAGE TO EQUIPMENT	COLLATERAL DAMAGE TO PERSONNEL
Non-Penetrating Projectiles	NO	YES	YES	NO	NO	UNLIKELY	UNLIKELY
Flash-Bang Devices	NO	POSSIBLE	YES	NO	NO	UNLIKELY	POSSIBLE
Lacrimators & Sternutators	CWC?	YES	YES	POSSIBLE	NO	NO	POSSIBLE
Electric Stunners	NO	POSSIBLE	POSSIBLE	NO	NO	NO	NO
Water Cannons	NO	POSSIBLE	YES	NO	NO	POSSIBLE	UNLIKELY
Vortex Ring Projectors	POSSIBLE	INDIRECT	INDIRECT	NO	NO	POSSIBLE	POSSIBLE
Tranquilizer Dart Guns	CWC?	RARELY	YES	NO	NO	NO	UNLIKELY
Infrasound Projectors	NO	INDIRECT	UNKNOWN	NO	NO	YES	YES
Sensor Aperture Coatings	NO	INDIRECT	INDIRECT	POSSIBLE	YES	UNLIKELY	UNLIKELY
Obscurants and Smokes	NO	RARELY	RARELY	POSSIBLE	NO	UNLIKELY	UNLIKELY
Laser Dazzling Weapons	U.S. POLICY	INDIRECT	YES	NO	NO	POSSIBLE	POSSIBLE
Isotropic Radiators	NO	INDIRECT	POSSIBLE	NO	NO	POSSIBLE	YES
Bucha Strobes	NO	NO	RARELY	NO	NO	NO	UNLIKELY
Microwave Projectors	NO	YES	UNKNOWN	NO	NO	UNLIKELY	POSSIBLE
Conductive Strand Chaff	NO	INDIRECT	INDIRECT	YES	YES	YES	INDIRECT
Metal Embrittlement Agents	CWC?	INDIRECT	INDIRECT	YES	YES	POSSIBLE	INDIRECT
Supercaustics & Superacids	CWC?	YES	YES	YES	YES	POSSIBLE	INDIRECT
Calmative Agents	CWC?	UNLIKELY	NO	NO	NO	NO	YES
Traction Modification Agents	NO	POSSIBLE	POSSIBLE	YES	POSSIBLE	POSSIBLE	POSSIBLE
Tire Deflation Devices	NO	INDIRECT	INDIRECT	NO	NO	POSSIBLE	UNLIKELY
Polymer Modification Agents	NO	POSSIBLE	POSSIBLE	YES	YES	POSSIBLE	INDIRECT
Foams	NO	UNLIKELY	UNLIKELY	YES	YES	UNLIKELY	UNLIKELY
Combustion Alteration Agents	NO	POSSIBLE	POSSIBLE	YES	YES	POSSIBLE	INDIRECT
Filter-clogging Agents	NO	POSSIBLE	POSSIBLE	YES	YES	POSSIBLE	POSSIBLE
Entanglement Devices	NO	POSSIBLE	POSSIBLE	NO	POSSIBLE	POSSIBLE	UNLIKELY
Biological Fuel-Eaters	BWC?	INDIRECT	INDIRECT	YES	YES	YES	NO
Malodorants	CWC?	UNLIKELY	UNLIKELY	POSSIBLE	YES	NO	YES

BWC – Biological Weapons Convention CWC – Chemical Weapons Convention

Figure K-2. Applications of Nonlethal Weapons.

	POTENTIAL APPLICATION									
NONLETHAL TECHNOLOGY	SUBDUE SINGLE PERSONS	SUBDUE LARGE GROUPS	DISPERSE/ DISRUPT CROWDS	ASSIST FORCED ENTRY	DISRUPT PERSONNEL MOBILITY	STOP MOVING VEHICLES	DAMAGE CRITICAL ELECTRONICS	DAMAGE CRITICAL STRUCTURES	NEGATE SENSOR FUNCTION	NEGATE POWER SYSTEM
Non-Penetrating Projectiles	YES	YES	YES	NO	POSSIBLE	UNLIKELY	UNLIKELY	NO	UNLIKELY	NO
Flash-Bang Devices	YES	POSSIBLE	POSSIBLE	YES	NO	NO	NO	NO	NO	NO
Lacrimators & Sternutators	YES	YES	YES	YES	INDIRECT	NO	NO	NO	NO	NO
Electric Stunners	YES	NO	UNLIKELY	NO	UNLIKELY	NO	NO	NO	NO	NO
Water Cannons	YES	YES	YES	NO	YES	POSSIBLE	POSSIBLE	NO	POSSIBLE	UNLIKELY
Vortex Ring Projectors	YES	NO	UNLIKELY	POSSIBLE	YES	NO	POSSIBLE	NO	NO	NO
Tranquilizer Dart Guns	YES	NO	NO	POSSIBLE	NO	NO	NO	NO	NO	NO
Infrasound Projectors	YES	YES	YES	POSSIBLE	INDIRECT	NO	POSSIBLE	POSSIBLE	NO	UNLIKELY
Sensor Aperture Coatings	NO	NO	NO	POSSIBLE	NO	POSSIBLE	NO	NO	YES	NO
Obscurants and Smokes	NO	NO	POSSIBLE	POSSIBLE	LIMITED	UNLIKELY	NO	NO	YES	NO
Laser Dazzling Weapons	YES	POSSIBLE	POSSIBLE	POSSIBLE	NO	POSSIBLE	NO	NO	YES	NO
Isotropic Radiators	POSSIBLE	YES	POSSIBLE	NO	NO	NO	NO	NO	YES	NO
Bucha Strobes	YES	POSSIBLE	POSSIBLE	NO	NO	NO	NO	NO	NO	NO
Microwave Projectors	POSSIBLE	POSSIBLE	POSSIBLE	POSSIBLE	INDIRECT	YES	YES	NO	POSSIBLE	POSSIBLE
Conductive Strand Chaff	NO	NO	NO	NO	NO	NO	POSSIBLE	NO	NO	YES
Metal Embrittlement Agents	NO	NO	NO	POSSIBLE	INDIRECT	POSSIBLE	POSSIBLE	YES	POSSIBLE	POSSIBLE
Supercaustics & Superacids	NO	NO	NO	POSSIBLE	NO	POSSIBLE	YES	YES	POSSIBLE	POSSIBLE
Calmative Agents	YES	YES	POSSIBLE	YES	NO	NO	NO	NO	NO	NO
Traction Modification Agents	NO	NO	POSSIBLE	NO	YES	YES	NO	NO	NO	NO
Tire Deflation Devices	NO	NO	NO	NO	LIMITED	YES	NO	NO	NO	NO
Polymer Modification Agents	NO	NO	NO	NO	NO	YES	YES	POSSIBLE	NO	POSSIBLE
Foams	YES	UNLIKELY	YES	NO	YES	POSSIBLE	UNLIKELY	POSSIBLE	NO	NO
Combustion Alteration Agents	NO	NO	NO	NO	NO	YES	NO	NO	NO	INDIRECT
Filter-clogging Agents	NO	NO	NO	NO	INDIRECT	YES	INDIRECT	INDIRECT	NO	NO
Entanglement Devices	YES	POSSIBLE	UNLIKELY	NO	YES	POSSIBLE	NO	POSSIBLE	NO	NO
Biological Fuel-Eaters	NO	NO	NO	NO	NO	YES	NO	NO	NO	INDIRECT
Malodorants	YES	YES	YES	POSSIBLE	LIMITED	NO	NO	NO	NO	NO

APPENDIX L. RELEVANT ARMS CONTROL TREATIES

Treaties, Conventions, Protocols, and Agreements

Affairs between nations that require mutual understanding and acceptance of specific rules or modes of action are traditionally governed by negotiated and signed formal documents. These documents are generally referred to as "treaties", although in the legalistic language of diplomacy they may be given other specific titles as appropriate to the nature of the document. It is not possible to truly understand the technological possibilities available to some states but not to others without learning about the various "arms control" and "non-proliferation" agreements that define "legal" vs. "illegal" behavior on the international scene. It is not possible to review every agreement relating to the laws and conduct of war. The author has attempted to discuss those that impact on one or more of the vulnerabilities identified in the body of this work. The relevant agreements may be treaties with full national and international ramifications or they may be less-binding documents that merely express the desires of two or more nations (or possibly only the desires of their negotiators). The language is important. For this reason the author has presented definitions for a number of diplomatic terms that the reader is likely to encounter in the course of his review of arms control negotiations [167].

DIPLOMATIC DOCUMENT DEFINITIONS

Treaty	*A contract in writing between two or more political authorities, formally signed by duly authorized representatives and usually ratified by the law-making authority of each state.*
Protocol	*1. A preliminary memorandum often formulated and signed by diplomatic negotiators as a basis for a final convention or treaty.* *2. An annex to a treaty giving supplemental data relating to it.*
Convention	*An agreement between states for the regulation of matters affecting all of them. Conventions are typically both signed and ratified.*
Agreement	*An arrangement as to a course of action.*
Accord	*A formal reaching of agreement.*
Regime	*A mode of rule or government. In practice, an agreed upon way of conducting governmental affairs between nations that is not prescribed by treaty nor ratified by the respective legislative bodies.*
Resolution	*A formal expression of opinion, will, or intent voted by an official body or assembled group.*

Agreed Statement *A formal declaration of accord on one or more specific points. These are issued at the conclusion of a round of negotiation to affirm those points on which agreement has been reached even though complete agreement on all issues has not.*

Memorandum *An informal diplomatic communication.*

Accession *The act by which one nation becomes party to an agreement already in force between other states.*

Ratify *To approve and sanction formally. Usually this requires legislative action.*

Sanction
1. *v.t. To give effective or authoritative approval or consent to.*
   n. Explicit or official approval, permission, or ratification.
2. *n. An economic or military coercive measure adopted usually by several nations in concert for forcing a nation violating international law to desist or yield to adjudication.*

Succession *The process whereby a new state that has gained its independence from a parent state, or a new government that has taken power from a former government, becomes bound by any or all prior treaties or agreements made by the former state or government. Succession is seldom automatic although it is often assumed. It is best accomplished with a formal, signed document. Without a formal declaration of succession, an unprincipled state could disregard any prior treaty whenever it pleased. It could claim that those prior agreements were made by a government which did not legitimately represent the people of the new state.*

Reservation *An expressed exception or qualification to part of a formal document. A state may generally agree with a treaty or other document and sign and/or ratify that document, but disagree with one or points of that document. When a state makes a reservation when it signs a document, all points of that document become binding on the state, <u>except</u> the point or point explicitly described in the reservation. For example, a state may make a reservation about the absolute non-use of chemical weapons in war, by reserving the right to use chemical weapons in defense if an attacking state has used chemical weapons first.*

Declaration *A formal statement made by one or more states that amplifies or clarifies one or more points of a formal document. The declaration is attached to a formal document at the time the declaring state signs the document. The declaration is not binding on any other state. A declaration define exactly what the declaring state assumes or means by specific terminology that is used in the document. For example, a state may declare that the term "chemical warfare agents" does <u>not</u> include "riot control chemicals".*

In the following sections we will discuss many of the international agreements that directly affect the proliferation of weapons of mass destruction. A more or less comprehensive list of such agreements is given in Table L-1. The major agreements will be discussed in some detail. For each of this agreements we will describe the following items: dates on which the United States signed and ratified the treaty, other important signatories, the date the treaty entered into force, and a brief discussion of each of the important provisions and implications of the agreement. Minor agreements will be discussed in enough detail that the reader will know the subject content and relevance of each agreement.

For none of the agreements will point-by-point or paragraph-by-paragraph analyses be presented. Complete texts and in-depth analyses of most of the "treaties" described in subsequent sections of this chapter can be found at the World Wide Web (Internet) site of the State Department's Bureau of Arms Control. That site can be reached at the URL:

http://www.state.gov/www/global/arms/bureau_ac/treaties_ac.html

Specific URL references will be given for each "treaty" when it is discussed. An alternate source of the complete texts is the book Arms Control and Disarmament Agreements published for the ACDA by the Government Printing Office [168]

Table L-1. International agreements affecting proliferation of WMD. The agreements are listed chronologically by the date the U.S. signed the agreement.

Protocol for the Prohibition of the Use in War of Asphyxiating, Poisoning or Other Gases, and Bacteriological Methods of Warfare **(The Geneva Protocol)**
U.S. signed 17 Jun 1925; U.S. ratified 22 Jan 1975; Entry into force 8 Feb 1928

The Antarctic Treaty
U.S. signed 1 Dec 1959; U.S. ratified 18 Aug 1960; Entry into force 23 Jun 1961

Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water **(Limited Test Ban Treaty)**
U.S. signed 5 Aug 1963; U.S. ratified 7 Oct 1963; Entry into force 10 Oct 1963

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies **(Outer Space Treaty)**
U.S. signed 27 Jan 1967; U.S. ratified 24 May 1967; Entry into force 10 Oct 1967

Treaty for the Prohibition of Nuclear Weapons in Latin America **(Treaty of Tlatelolco)**
Signed 14 Feb 1967; U.S. signed both protocols; Entry into force 22 Apr 1968

Treaty on the Non-Proliferation of Nuclear Weapons **(Non-Proliferation Treaty)**
U.S. signed 1 Jul 1968; U.S. ratified 24 Nov 1969; Entry into force 5 Mar 1970

Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Seabed and the Ocean Floor and in the Subsoil Thereof **(Seabed Treaty)**
U.S. signed 11 Feb 1971; U.S. ratified 26 Apr 1972; Entry into force 18 May 1972

Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction **(Biological & Toxin Weapons Convention)**
U.S. signed 10 Apr 1972; U.S. ratified 22 Jan 1975; Entry into force 26 Mar 1975

Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems **(ABM Treaty)**
U.S. signed 26 May 1972; U.S. ratified 30 Sep 1972; Entry into force 3 Oct 1972

Interim Agreement Between the United States of America and the Union of Soviet Socialist Republics on Certain Measures with Respect to the Limitation of Strategic Offensive Arms **(SALT I)**
U.S. signed 26 May 1972; U.S. ratified 30 Sep 1972; Entry into force 3 Oct 1972
SALT I expired in October 1977.

Convention on Prohibition or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to have Indiscriminate Effects (and Protocols Thereto) **(Convention on Conventional Weapons)**
U.S. signed 8 April 1982; U.S. ratified Protocols I & II in March 1995; Entry into force 2 Dec 1983

Table L-1 (continued). International agreements affecting proliferation of WMD.

Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Underground Nuclear Weapon Tests (and Protocol Thereto) **(Threshold Test Ban Treaty)**
U.S. signed 3 Jul 1974; U.S. ratified 8 Dec 1990; Entry into force 11 Dec 1990

Treaty Between the United States of America and the Union of Soviet Socialist Republics on Underground Nuclear Explosions for Peaceful Purposes **(Peaceful Nuclear Explosions Treaty)**
U.S. signed 3 Jul 1974; U.S. ratified 8 Dec 1990; Entry into force 11 Dec 1990

Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques **(Environmental Modification Convention)**
U.S. signed 18 May 1977; U.S. ratified 13 Dec 1979; Entry into force 17 Jan 1980

Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Strategic Offensive Arms, Together with Agreed Statements and Common Understandings Regarding the Treaty **(SALT II)**
U.S. signed 18 Jun 1979; U.S. did not ratify, but did not reject; Observance required.

The Convention on the Physical Protection of Nuclear Material
U.S. signed 3 Mar 1980; U.S. ratified 4 Sep 1981; Entry into force 8 Feb 1987

South Pacific Nuclear Free Zone Treaty **(Treaty of Rarotonga)**
Signed 6 Aug 1985; Entry into force 11 Dec 1986;

Missile Technology Control Regime **(MTCR)**
Established 16 Apr 1987; Not a formal treaty.

Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Elimination of their Intermediate Range and Shorter-Range Missiles **(INF Treaty)**
U.S. signed 8 Dec 1987; U.S. ratified 1 Jun 1988; Entry into force 1 Jun 1988

Agreement on Destruction and Non-Production of Chemical Weapons and on Measures to Facilitate the Multilateral Convention on Banning Chemical Weapons
U.S. signed 1 Jun 1990; Ratification not required; Entry into force 1 Jun 1990

Treaty on Conventional Armed Forces in Europe **(CFE Treaty)**
U.S. signed 19 Nov 1990; U.S. ratified 30 Oct 1992; Entry into force 9 Nov 1992

The Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms **(START I)**
U.S. signed 31 Jul 1991; U.S. ratified 1 Oct 1992; Entry into force 5 Dec 1994

Treaty on Open Skies
U.S. signed 24 Mar 1992; U.S. ratified 3 Dec 1993; Entry into force awaiting ratification by the governments of the Ukraine, Belarus, and the Russian Federation.

Table L-1 (continued). International agreements affecting proliferation of WMD.

The Treaty Between the United States of America and the Russian Federation on Further Reduction and Limitation of Strategic Offensive Arms **(START II)**
U.S. signed 3 Jan 1993; U.S. ratified 26 Jan 1996; Russian Duma ratified 14 April 2000.
Entry into force should occur shortly if it has not already occurred.

Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction **(Chemical Weapons Convention)**
U.S. signed 13 Jan 1993; U.S. ratified 25 Apr 1997; Entry into force 29 Apr 1997

South East Asian Nuclear-Weapon-Free Zone Treaty **(Treaty of Bangkok)**
Signed 15 Dec 1995; U. S. not ratified Protocol; Entry into force 27 Mar 1997

The African Nuclear-Weapon-Free Zone Treaty **(Treaty of Pelindaba)**
Signed 11 Apr 1996; Entry into force awaits sufficient ratifications.

The Comprehensive Nuclear Test-Ban Treaty **(CTBT)**
U.S. signed 24 Sep 1996; U.S. ratification currently under Congressional review.

Fissile Material Production Cut-off Treaty
Currently under negotiation.

Strategic Arms Reduction Talks III **(START III)**
Negotiations should begin after START II enters into force.

Central Asian Nuclear-Weapon-Free Zone Treaty
Currently under negotiation.

The Hague Conventions and the Geneva Protocol

On 29 November 1868 an International Military Commission assembled in St. Petersburg, Russia to determine if it was practical to ban certain kinds of weapons to "alleviate as much as possible the calamities of war". The ***"Declaration of St. Petersburg"*** [237] provided that States' Parties would not employ arms which uselessly aggravate the sufferings of disabled men, or render their death inevitable. The declaration specifically renounced the employment of any projectile of a weight less than 400 grams, which is either explosive or charged with fulminating or inflammable substances. Although of limited significance, the St. Petersburg Declaration set the tone for later arms control agreements.

At the invitation of Tsar Nicholas II of Russia, and hosted by Queen Wilhelmina of the Netherlands, The First International Peace Conference convened in The Hague on 18 May 1899.[169] This meeting was unique in that for the first time nations gathered together not to settle an ongoing war but to try to build a lasting peace. After ten weeks of negotiations between 25 attending nations, on 29 July 1899 the conference adopted a number of agreements including:

* "Convention for the Pacific Settlement of International Disputes"
* "Convention with Respect to the Laws and Customs of War on Land"
* Several other Declarations.

The second of these conventions is of significance to proliferation. The **Second Hague Convention (1899)**, formally called the ***"Convention with Respect to the Laws and Customs of War on Land"***, was [170]:

* Signed on 29 July 1899 by Germany, United States, Russia (tsarist), France, Italy, United Kingdom, Austria, Hungary, and many other states.
* The Convention entered into force on 4 September 1900.

The Second Hague Convention of 1899 contained a large number of provisions. Among these were provisions relating to:

* Qualifications of belligerents subject to the Laws of War,
* Humane treatment of prisoners of war,
* Care of the sick and wounded,
* Conduct of hostilities,
* Spies,
* Flags of Truce,
* Surrender,
* Armistices,
* Military authority over hostile territory,
* Internment of belligerents in neutral countries.

The provision relating to the conduct of hostilities prohibits (among other things):

* Employment of poison or poisoned arms,
* Employment of arms, projectiles, or material of a nature to cause superfluous injury.

One separate ***"Declaration on the Use of Bullets Which Expand or Flatten Easily in the Human Body"*** was signed on 29 July 1899.[238] This declaration explicitly prohibited the recently developed "dum-dum" bullets designed to cause excessive damage to internal organs and tissues. A second ***"Declaration on the Use of Projectiles the Object of Which is the Diffusion of Asphyxiating or Deleterious Gases"***, also passed on 29 July 1899 [239], was the first serious attempt at banning chemical weapons, even though these weapons had not yet been used in warfare.

A Second International Peace Conference was held at The Hague in 1907. Even more nations participated in this second conference than participated in the first. On 18 October 1907, the conference adopted eleven different conventions. Among these was a revision of the Second Hague Convention. The **Hague Convention IV of 1907**, i.e., the ***"Convention Respecting the Laws and Customs of War on Land"*** was [171]:

* Signed on 18 October 1907 by Germany, United States, Russia (tsarist), France, Italy, United Kingdom, Austria, Hungary, and many other states.
* The Convention entered into force on 16 January 1910.

The provisions of the revised Second Hague Convention of 1907 were essentially the same as those of the 1899 version. Language was altered to clarify meanings. The provision relating to the conduct of hostilities prohibits:

* Employment of poison or poisoned arms,
* Employment of arms, projectiles, or material calculated to cause unnecessary suffering.
* The attack or bombardment of towns, villages, dwellings, or buildings which are undefended [and not being used for military purposes].

In sieges and bombardments steps must be taken to spare buildings dedicated to religion, art, science, charitable purposes, historic monuments, hospitals, and places for the collection of sick and wounded, provided they are not being used for military purposes.

Neither version of the Second Hague Convention contained any enforcement or verification provisions. Essentially, the convention represents a statement of good intent. However, any country that decided to violate any provision could do so with impunity. They might earn the condemnation of other countries, but that would be the only significant penalty. To say that the convention did no real good is unfair. There is evidence that Britain delayed developing and using chemical weapons in World War I until after the Germans used them at Ypres, because in the words of Winston Churchill, "we were confined to a limited sphere of International Law till Germany forced us to take reprisals in the matter of poisonous gas" [172]. That is, they did not want to be the first to violate the Hague Convention. Nevertheless, once the Germans used poison gas, everyone used poison gas; and the poison gas provisions of the Hague Convention ceased to have any meaning or value.

Several other conventions adopted at the second Hague peace conference limit military technology options in warfare. The **Hague Convention III of 1907** or ***"The Convention Relative to the Opening of Hostilities"*** was signed on 18 October 1907.[240] This convention requires that hostilities "must not commence without previous and explicit warning, in the form either of a reasoned declaration of war or of an ultimatum with condition declaration of war. The fact that the Japanese attack on Pearl Harbor preceded by 35 minutes the delivery of such an ultimatum to the U. S. government (due to delays in the Japanese Embassy) was a major factor is stirring America to war against the Japanese. It also was a factor in U. S. insistence on unconditional surrender (that ultimately led the U. S. use of atomic weapons).

The **Hague Convention XI of 1907** or ***"The Convention Relative to Certain Restrictions With Regard to the Exercise of the Right of Capture in Naval War"*** was signed on 18 October 1907. [241] Among other things this convention exempted "vessels used exclusively for fishing along the coast or small boats employed in local trade" from captures as long as those vessels take no part in any hostilities. The Contracting Powers also agreed not to take advantage of the harmless character of such vessels in order to use them for military purposes while preserving their peaceful appearance. Vessels charged with religious, scientific, or philanthropic missions are likewise exempt from capture. The Hague Convention XI of 1907 effectively prohibits the use of the civilian fishing fleet and/or coastal commerce fleets from acting as armed auxiliaries to the military. However, since these vessels do have the right to carry certain kinds of weapons for defense against piracy and since virtually every vessel has long-range radios, GPS, and navigational radars, it is probably impossible to enforce this convention. However, in the absence of proven hostile intent, States must recognize these vessels as non-hostile and avoid attacking or capturing them.

The **Hague Convention VIII of 1907** or ***"The Convention Relative to the Laying of Automatic Submarine Contact Mines"*** was also signed on 18 October 1907. [242] The primary provisions of this convention forbid:

* Laying unanchored automatic contact mines, except when they are so constructed as to become harmless one hour at most after the person who laid them ceases to control them.
* Laying anchored automatic contact mines which do not become harmless as soon as they have broken loose from their moorings.
* Using torpedoes that do not become harmless when they have missed their mark.
* Laying automatic contact mines of the coast and ports of the enemy, with the sole object of intercepting commercial shipping.

Provisions also require:

* Rendering harmless deployed mines within a limited time.
* Notifying all governments and ship owners of the danger zones as soon as those areas cease to be under surveillance.
* At the end of hostilities, removing all mines that each power has laid off its own shores notifying the other belligerents of the locations of all mines laid off the others' shores so that the other belligerents may safely remove them.

The Hague Convention VIII of 1907 and the Seabed Treaty (discussed later) are the only two significant treaties which address the deployment of unattended weapons (such as mines) at sea.

The **Geneva Protocol** was the first major international agreement attempting to ban new forms of technological warfare. Note: the Geneva Protocol is to be distinguished from the Geneva Conventions of 1949 that addressed treatment of prisoners of war. Formally titled the ***"Protocol for the Prohibition of the Use in War of Asphyxiating, Poisoning, or Other Gases, and Bacteriological Methods of Warfare"***, the Geneva Protocol was [173]:

* Signed on 17 June 1925 by the United States, Germany, France, United Kingdom, Italy, Japan, and many other states.
* Ratified by the U. S. President on 22 January 1975
* Protocol entered into force on 8 February 1928.

Countries of special note that have ratified or acceded to the Geneva Protocol include:

Argentina	Belarus	Brazil
Bulgaria (ab)	Burma (ab)	Cambodia
Canada (ab)	China (ab)	Cuba
Czechoslovakia (b)	Egypt	France (ab)
Germany	India (ab)	Indonesia
Iran	Iraq (ab)	Israel (ab)
Japan	North Korea	Republic of Korea (ab)
Libya (bd)	Malaysia	Mexico
Pakistan	Philippines	Romania (ab)
Russian Federation (ab)?	South Africa (ab)	Sudan
Syria (d)	Taiwan	United Kingdom (ab)
United States (c)	Vietnam	Yugoslavia

Countries of special note which have not signed or acceded to the Geneva Protocol include:

- El Salvador has signed but not ratified the Protocol
- The Russian Federation has not formally acknowledged its succession to this agreement.

  Only Belarus of the former USSR has declared succession to this agreement
- The successor states to the former socialist republic of Yugoslavia have not declared succession to this agreement.

The entire Geneva Protocol is less than a page in length. It contains three principle provisions. Each state ratifying or acceding to the Protocol shall:

* Accept the prohibition on the use in war of asphyxiating, poisonous or other gases, and of all analogous liquids, materials, or devices.
* Accept the prohibition on the use in war of bacteriological methods of warfare.
* Exert every effort to induce other states to accede to the present Protocol.

Many ratifiers expressed one or more reservations to the protocol. The letters in parentheses following a country's name identify the specific reservations made. The reservations are:

a - binding only as regards to relations with other parties.

b - to cease to be binding in regard to any enemy States whose armed forces or allies do not observe provisions.

c - to cease to be binding as regards use of chemical agents with respect to any enemy State whose armed forces or allies do not observe provisions.

d - does not constitute recognition of or involve treaty relations with Israel.

As an arms control agreement, the Geneva Protocol has been both a success and a failure. Its success lies in the fact that even during the largest and bloodiest war in human history there were few if any incidents of chemical weapons use (and most of those were by a non-ratifier of the Protocol). Many government and military leaders believed that the Protocol outlawed the use of chemical weapons. No one (including Hitler, it seems) was willing to become the first "outlaw". The incidents of use other than during World War II have also been few in number. Another measure of success was that it paved the way for both the Biological & Toxin Weapons Convention and the Chemical Weapons Convention in the last part of this century.

The Geneva Protocol's failure lies in that it did little to stop the proliferation of chemical weapons. It addressed only the use of chemical and bacteriological weapons. The Protocol says nothing about not acquiring, not improving, not manufacturing, not selling, nor destroying existing chemical weapons. Many countries openly reserved the right to retaliate with chemical weapons if they were attacked by other countries using chemical weapons.

The protocol has two other main flaws. First, it lacks a verification provision. There is no stated legal right for one state to investigate on the accused's sovereign territory any allegations of the use of chemical weapons by the accused against another state. Second, it lacks any punitive provision. Even if it is proved that State A (a ratifier of the Protocol) used chemical weapons in war against State B, there is no penalty prescribed. In principle, State A cannot be seriously investigated for potential violations of the Protocol, and even if it admits violations, it cannot be punished for those violations. In short, the Geneva Protocol is a statement of good intent, but not seriously binding or limiting on the behavior between states.

It should be noted that the United States pushed for the adoption of the Geneva Protocol, signed it, and then failed to ratify it for 50 years. The details are not entirely clear. It appears that there was extensive lobbying against the Protocol when it first came to the Senate for ratification. The arguments used are not available to the author. When it failed on the first try, ratifying the Protocol was placed on the back burner, as business more pressing needed doing. Later, the Protocol was seen to have no obvious effect on disarmament and the United States military had turned to view chemical weapons as another element of its arsenal of deterrence. It languished until the 1970's when new arms control incentives required that the issue of non-ratification be put to rest permanently.

Chemical Weapons Convention

The **Chemical Weapons Convention** (or CWC) is the primary international agreement for limiting the use of chemical weapons. Formally titled the ***"Convention on the Prohibition of the Development, Production and Stockpiling of Chemical Weapons and on Their Destruction"*** , the CWC was [174]:

* Signed on 13 January 1993 by the United States, United Kingdom, Soviet Union, and many other states
* Ratified by the U. S. President on 25 April 1997
* Treaty entered into force on 29 April 1997

Countries of note that have signed & ratified or acceded to the CWC include:

Algeria	Argentina	Australia
Belarus	Bosnia & Herzegovina	Brazil
Bulgaria	Canada	China
Croatia	Cuba	Czech Republic
Fed. Rep. Yugoslavia	France	Germany
India	Indonesia	Iran
Japan	Kazakhstan	Laos
Malaysia	Mexico	Pakistan
Republic of Korea	Romania	Russian Federation
Slovak Republic	Slovenia	South Africa
Sudan	Ukraine	United Kingdom
United States	Vietnam	

Countries that have signed but not ratified the CWC include:

Afghanistan	Bahamas	Bhutan
Cambodia	Cape Verde	Chad
Comoros	Congo	Dem. Rep of the Congo
Djibouti	Dominica	Dominican Republic
Gabon	Grenada	Guatemala
Guinea-Bissau	Haiti	Honduras
Israel	Jamaica	Kyrgyzstan
Liberia	Madagascar	Marshall Islands
Myanmar (Burma)	Nauru	Rwanda
St. Kitts & Nevis	Samoa	Sierra Leone
Thailand	Uganda	United Arab Emirates
Yemen	Zambia	

Countries of special note that have not signed or acceded to the CWC include:

Angola	Egypt	Iraq
Lebanon	Libya	Mozambique
North Korea	Somalia	Syria
Taiwan (not permitted to sign due to PRC)		

In the CWC, the following definitions are used.

"**Chemical weapons**" means together or separately, (a) toxic chemicals and their precursors, except where intended for purposes not prohibited under this Convention, as long as the types and quantities are consistent with such purposes, (b) munitions and devices, specifically designed to cause death or other harm through the toxic properties of those toxic chemicals specified in (a), which would be released as a result of the employment of such munitions and devices, and (c) any equipment specifically designed for use directly in connection with the employment of munitions and devices specified in (b).

“**Toxic chemicals**” means any chemical which through its chemical action on life processes can cause death, temporary incapacitation, or permanent harm to humans or animals. *This includes all such chemicals, regardless of their origin or their method of production, and regardless of whether they are produced in facilities, in munitions or elsewhere.*

“**Precursor**” means any chemical reactant that takes part at any stage in the production by whatever method of a toxic chemical. This includes any key component of a binary or multicomponent chemical system.

“**Key component of binary or multicomponent chemical systems**” means the precursor that plays the most important role in determining the toxic properties of the final product and reacts rapidly with other chemicals in the binary or multicomponent system.

“**Old chemical weapons**” means chemical weapons produced before 1925, or produced in the period 1925 and 1946 that have deteriorated to such extent that they can no longer be used as chemical weapons.

“**Abandoned chemical weapons**” means chemical weapons, including old chemical weapons, abandoned by a State after 1 January 1925 on the territory of another State without the consent of the latter.

“**Riot control agent**” means any chemical not listed in one of the Schedules of the Annex on Chemicals (see below), which can produce rapidly in humans sensory irritation or disabling effects which disappear within a short time following termination of exposure.

“**Chemical weapons production facility**” means any equipment, as well as any building housing such equipment, that was designed, constructed, or used at any time since 1 January 1946 (i) as part of the stage in the production of chemicals where material flows would contain, when the equipment is in operation, any chemical listed in Schedule 1 of the Annex on Chemicals or any other chemical that has no use above 1 tonne per year for purposes not prohibited under this Convention, but can be used for chemical weapons purposes, or (ii) for filling chemical weapons.

“**Purposes not prohibited under this convention**” include industrial, agricultural, research, medical, pharmaceutical, or other peaceful purposes; protective purposes related to protection against toxic chemicals or chemical weapons; military purposes not connected with the use of chemical weapons and not dependent on the use of the toxic properties of chemicals as a method of warfare; and law enforcement including domestic riot control purposes.

“**Production capacity**” means the annual quantitative potential for manufacturing a specific chemical based on the technological process used.

The primary provisions of the CWC include:

Each State Party to this Convention undertakes never under any circumstance:

* To develop, produce, otherwise acquire, stockpile or retain chemical weapons, or transfer, directly or indirectly, chemical weapons to anyone.
* To use chemical weapons.
* To engage in any military preparations to use chemical weapons.

Each State Party undertakes:

* To destroy chemical weapons it owns or possesses, or that are located in any place under its jurisdiction or control, in accordance with the provisions of this Convention.

NOTE: in the following, “possess” shall mean “owns or possesses, or that are located any place under its jurisdiction or control”.

* To destroy all chemical weapons it abandoned on the territory of another State Party.
* To destroy any chemical weapon production facilities it possesses.
* Not to use riot control agents as a method of warfare.

The Convention contains provision for a number of declarations to be made. Thus, each State Party shall submit to the Organization for the Prohibition of Chemical Weapons, the following declarations in which it shall:

* Declare whether it possesses any chemical weapons.
* Specify the location, aggregate quantity and detailed inventory of chemical weapons it possesses.
* Report any chemical weapons on its territory that are possessed by another State.
* Provide its general plan for the destruction of chemical weapons it possesses.
* Declare whether there are abandoned chemical weapons on its territory and provide all available information.
* Declare whether it has abandoned chemical weapons on the territory of other States and provide all available information.
* Specify any chemical weapons production facility that it possesses or has had under its possession at any time since 1 January 1946.
* Provide its general plan for destruction of any chemical weapon production facility it possesses.
* Specify the precise location, nature and general scope of activities of any facility or establishment under its possession that has been designed, constructed, or used since 1 January 1946 primarily for development of chemical weapons. Such declaration shall include laboratories and test and evaluation sites.

The declaration provisions shall not apply to any chemical weapons buried on its territory before 1 January1977 and which remain buried, or which had been dumped at sea before 1 January 1985.

The destruction of chemical weapons must be carried out in a safe and environmentally friendly manner. Open pit burning, land burial, or dumping in any body of water are specifically prohibited. Any chemical weapons previously buried on its own territory (before 1 January 1977) or dumped at sea (before 1 January 1985) may remain untouched. If a State elects to recover such weapons they must be declared and destroyed like all other chemical weapons.

States Parties to this convention are required to destroy all chemical weapons within 10 years. The rate of destruction shall be according to the schedule:

* Begin destruction of Schedule 2 and 3 chemical weapons within 1 year
* Test the first Schedule 1 destruction facility within 2 years
* Destroy 1% of Schedule 1 chemical weapons within 3 years
* Destroy 20% of Schedule 1 and 100% of Schedule 2 and 3 chemical weapons within 5 years
* Destroy 45% of Schedule 1 chemical weapons within 7 years
* Destroy 100% of Schedule 1 chemical weapons within 10 years.

It remains to be seen whether either the United States or the Russian Federation will be able to complete destruction of their massive chemical arsenals according to this timetable.

After completion of destruction, the chemical industries of the States Parties will be subject to production limitation on certain chemicals. For Schedule 1 chemicals:

> The national aggregate of all Schedule 1 chemicals may not exceed 1 tonne at any given time. Production data must be declared for all facilities producing any quantity of these chemicals. A single small-scale production facility with a maximum annual production of up to 1 tonne per year is permitted. All other facilities are limited to less than 10 kg per year production rate. Schedule 1 chemicals can only be transferred from one State Party to another State Party. An advance notification to the OPCW is required.

For Schedule 2 chemicals:

> Production, processing, consumption, import, and export data must be declared for all plant sites producing, processing, or consuming in excess of 1 kg per year for those chemicals in Schedule 2A marked with an asterisk, 100 kg per year for all other chemicals in Schedule 2A, or 1 tonne per year for all chemicals in Schedule 2B. The sites of all such plants must also be declared. The State Party will report national aggregate amounts of each Schedule 2 chemical produced, processed, consumed, imported, or exported. Import and Export quantities must be specified for each country involved. A State Party can only transfer Schedule 2 chemicals to another State Party.

For Schedule 3 chemicals:

> Production, import, and export data must be declared for plant sites producing Schedule 3 chemicals in excess of 30 tonnes per year. The sites of all such plants must also be declared. The State Party must report national aggregate amounts of each Schedule 3 chemical produced, imported, and exported, as well as quantitative data on the imports and exports for each country involved. Beginning in May 2002, the OPCW will consider restrictions on the transfer of Schedule 3 chemicals to States not party to the Convention.

For all other organic chemical sites:

> A State Party will have to declare all plant sites that produce aggregate quantities of discrete organic chemicals in excess of 200 tonnes per year. It must also declare the sites of plants producing more than 30 tonnes per year of any discrete organic chemical containing the elements phosphorus, fluorine, or sulfur.

Verification of compliance with this treaty will be performed by the Technical Secretariat of an Organization for the Prohibition of Chemical Weapons (OPCW). The OPCW will be headquartered in The Hague. It will be governed by a Conference of the States Parties which will meet on an annual basis. An Executive Council consisting of 41 representatives elected for 2-year terms among the Member States, has the day-to-day responsibility for supervising the activities of the OPCW.

The destruction of chemical weapons and the production of organic chemicals are subject to inspections to verify compliance with the Convention. Routine on-site inspection and possibly continuous monitoring shall be used to verify the compliance of the destruction of all chemical weapons and chemical weapon production facilities. Details of the inspection and monitoring are to be negotiated between the OPCW and each State. Routine on-site inspections will also be made of each industrial facility that produces, processes, consumes, imports, or export any of the

Scheduled chemicals that was declared to the OPCW by virtue of the quantities of chemical involved (as described above).

Any Member State has the right to request a challenge inspection. The purpose of a challenge inspection is to clarify and resolve any question in relation to a possible non-compliance with any of the provisions of the Convention. Any facility at any location in the territory or any other place under the jurisdiction or control of any other State Party. The Executive Council may abort any challenge inspection if by 3/4 majority decision it decides the request is abusive, frivolous, on non-consonant with the Convention. The Executive Council may sanction any State that it deems to be abusing the challenge inspection process. At least 12 hour advance warning must be given for challenge inspection. The inspected party is under the obligation to make all reasonable efforts to demonstrate compliance. However, it may invoke access delays and managed access to protect sensitive installations and confidential information unrelated to the Convention. The inspectors are obligated to use "only those methods necessary to provide sufficient relevant facts to clarify the concern of possible non-compliance". They are bound by a strict confidentiality policy not to acquire, record, or disclose any information not relevant to the concern that prompted the inspection.

A final right under the Convention is the right to assistance if chemical weapons are used against any State Party. That assistance may consist of detection equipment, protection equipment, decontamination equipment, medical antidotes and treatments, and advice on protective measures. The assistance shall be provided by other Member States according to their capabilities.

Compliance with the Convention can be mandated in two ways. If a non-compliance is proven, then the Conference of the States Parties may suspend the rights of the non-compliant State under the Convention. Basically, this means that transfers of Scheduled chemicals to any other State would be prohibited (a potentially serious impact on the chemical industry of the offending State). Particularly serious non-compliance can be referred to the United Nations General Assembly and the United Nations Security Council for potential action on a broader scale. The United Nations could impose penalties ranging from police action to widespread economic sanctions and embargo.

The chemical which are explicitly controlled under the CWC are defined in the Annex on Chemicals. The Annex has three schedules. Schedule 1 chemicals are highly lethal chemicals and their precursors. These chemicals include nerve agents of the tabun, sarin, and VX families, vesicants including mustards and lewisites, and two toxins (ricin and saxitoxin). These chemicals have almost no non-military applications. Schedule 2 chemicals are less lethal chemical warfare agents and precursors to Schedule 1 and 2 chemical warfare agents. These chemicals have some but limited use in industry. Schedule 3 chemicals include several World War I chemical warfare agents and a wide variety of precursors to more lethal chemical warfare agents. Schedule 3 chemicals invariably have considerable industrial applications, that make their total banning unacceptable. Details of all three Schedules are included in Table L-2 below.

Table L-2. Chemicals controlled under the Chemical Weapons Convention: Schedule 1.[174]

<u>SCHEDULE 1</u> - Major chemical warfare agents or their key final-stage precursors with little or no commercial use. All stocks except 1000 kg stored at one facility per country must be destroyed. This facility is subject to inspection.

A. TOXIC CHEMICALS:

* O-R1-R2-phosphonofluoridate — R1 # C10 including cycloalkyl; R2 = methyl, ethyl, n-propyl, isopropyl
  - *EXAMPLE:* Sarin or GB — O-Isopropyl methylphosphonofluoridate
  - Soman or GD — O-Pinacolyl methylphosphonofluoridate
* O-R1-N,N-di(R2)-phosphoramidocyanate — R1 # C10 including cycloalkyl; R2 = methyl, ethyl, n-propyl, isopropyl
  - *EXAMPLE:* Tabun or GA — O-Ethyl-N,N-dimethyl phosphoramidocyanidate
* O-R1-S-[2-N,N-di(R2)amino)ethyl]-R3-phosphonothiolate <u>and</u> alkylated or protonated salts — R1 # C10 including cycloalkyl; R2 = methyl, ethyl, n-propyl, isopropyl
  - *EXAMPLE:* VX O-Ethyl-S-[2-N,N-(diisopropylamino)ethyl]methylphosphonothiolate

SULFUR	* H	Bis(2-chloroethyl)sulfide
MUSTARDS	* Q	1,2-Bis(2-chloroethylthio)ethane
	* T	Bis(2-chloroethylthioethyl)ether
	*	Bis(2-chloroethylthio)methane
	*	1,3-Bis(2-chloroethylthio)-n-propane
	*	1,4-Bis(2-chloroethylthio)-n-butane
	*	1,5-Bis(2-chloroethylthio)-n-pentane
	*	2-chloroethylchloromethylsulfide
	*	Bis(2-chloroethylthiomethyl)ether
LEWISITES	* L-1	2-Chlorovinyldichloroarsine
	* L-2	Bis(2-chlorovinyl)chloroarsine
	* L-3	Tris(2-chlorovinyl)arsine
NITROGEN	* HN1	Bis(2-chloroethyl)ethylamine
MUSTARDS	* HN2	Bis(2-chloroethyl)methylamine
	* HN3	Tris(2-chloroethyl)amine

* Saxitoxin
* Ricin

B. PRECURSORS:

* R1-Phosphonyldifluoride — R1 = methyl, ethyl, n-propyl, isopropyl
  - *EXAMPLE:* DF — Methylphosphonic difluoride
* O-R1-O-[2-(N,N-di(R2)amino)ethyl]-R3-phosphonites <u>and</u> alkylated or protonated salts — R1 # C10 including cycloalkyl; R2, R3 = methyl, ethyl, n-propyl, isopropyl
  - *EXAMPLE:* QL — O-[2-(N,N-Diisopropylamino)ethyl]-O-ethyl methylphosphonite
* Chlorosarin — O-Isopropyl methylphosphonochloridate
* Chlorosoman O-Pinacolyl methylphosphonochloridate

Table L-2 (continued). Chemicals controlled under the Chemical Weapons Convention: Schedule 2.

<u>SCHEDULE 2</u> - Toxic chemicals with high potential for use as chemical warfare agents (or their key final-stage precursors) or key early-stage precursors to Schedule 1 chemicals with low to moderate commercial use. All quantities in excess of 100 kg (toxics) and 1000 kg (precursors) must be reported. Facilities are subject to inspection.

A. TOXIC CHEMICALS:

* Amiton	O,O'-Diethyl-S-[2-N,N-(diethylamino)ethyl]phosphorothiolate
* PFIB	1,1,3,3,3-Pentafluoro-2-(trifluoromethyl)-1-propene
* BZ(*)	3-Quinuclidinyl benzilate ((*) – BZ is subject to a special 1 kg limit for reporting)

B. PRECURSORS:

* Chemicals (except those in Schedule 1) containing a phosphorus atom bonded to a single methyl, ethyl, or propyl group but to no other carbons
EXEMPTED: Fonofo O-Ethyl-S-Phenyl-Ethylphosphonothiolothionate
* N,N-Di(R1)phosphoramidic dihalide R1 = methyl, ethyl, n-propyl, isopropyl
* O,O'-Di(R1)-N,N-di(R2)phosphoramidate R1, R2 = methyl, ethyl, n-propyl, isopropyl
* Arsenic trichloride
* Benzilic acid 2,2-Diphenyl-2-hydroxyacetic acid
* Quinuclidine-3-ol
* N,N-Di(R1)aminoethyl-2-chloride <u>and</u> protonated salts
R1 = methyl, ethyl, n-propyl, isopropyl
* N,N-Di(R1)aminoethan-2-ol <u>and</u> protonated salts
R1 = methyl, ethyl, n-propyl, isopropyl
* N,N-Di(R1)aminoethane-2-thiol <u>and</u> protonated salts
R1 = methyl, ethyl, n-propyl, isopropyl
EXEMPTED: N,N-Dimethylaminoethanol and protonated salts
N,N-Diethylaminoethanol and protonated salts
* Thiodiglycol Bis(2-hydroxyethyl)sulfide
* Pinacolyl alcohol 3,3-Dimethyl-butan-2-ol

Table L-2 (continued). Chemicals controlled under the Chemical Weapons Convention: Schedule 3.

SCHEDULE 3 - Toxic chemicals considered obsolete as chemical warfare agents or early stage precursors to any scheduled chemical with high commercial use. Facilities producing 30,000 kg/yr of any scheduled chemical must be declared. Facilities producing more than 200,000 kg/yr are subject to inspection.

A. TOXIC CHEMICALS:

* Phosgene (or Carbonyl dichloride)
* Cyanogen chloride
* Hydrogen Cyanide
* Chloropicrin (or Trichloronitromethane)

B. PRECURSORS:

* Phosphoryl chloride
* Phosphorus trichloride
* Phosphorus pentachloride
* Thionyl chloride
* Sulfur Monochloride
* Sulfur Dichloride
* Trimethyl phosphite
* Triethyl phosphite
* DMHP or Dimethyl hydrogen phosphite
* DEHP or Diethyl hydrogen phosphite
* Ethyldiethanolamine
* Methyldiethanolamine
* Triethanolamine

Biological & Toxin Weapons Convention

The **Biological and Toxin Weapons Convention** (or BTWC) is the primary international agreement for limiting the use of biological weapons. Formally titled the ***"Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction"***, the BTWC was [175]:

* Signed on 10 April 1972 by the United States, United Kingdom, Soviet Union, and many other states
* Ratified by the U. S. President on 22 January 1975
* Treaty entered into force on 26 March 1975

Countries of special note that have ratified or acceded to the BTWC include:

Argentina	Belarus	Bosnia & Herzegovina
Brazil	Bulgaria	Cambodia
China	Croatia	Cuba
Czech Republic	France	Germany
Hungary	India	Indonesia
Iran	Iraq	Japan
Republic of Korea	Laos	Libya
Malaysia	Mexico	Mongolia
North Korea	Pakistan	Romania
Russian Federation	Slovakia	Slovenia
South Africa	Taiwan	Ukraine
United Kingdom	United States	Vietnam
Yugoslavia		

Countries of special note that have signed but not ratified the BTWC include:

Burundi	Central African Republic	Cote d'Ivoire
Egypt	Gabon	Guyana
Haiti	Liberia	Madagascar
Malawi	Mali	Morocco
Myanmar (Burma)	Nepal	Somalia
Syria	Tanzania	United Arab Emirates

Countries of special note which have not signed or acceded to the BTWC include:

Algeria	Israel	Kazakhstan
Lithuania	Moldova	Taiwan (not permitted)

The principal provisions of the BTWC include:

Each State Party to this Convention undertakes:

* Never in any circumstances to develop, produce, stockpile or otherwise acquire or retain:
  (1) Microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective, or other peaceful purposes;
  (2) Weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict.
* To destroy, or divert to peaceful purposes, all agents, toxins, weapons, equipment and means of delivery which are in its possession or under its jurisdiction or control.

* Not to transfer to any recipient whatsoever, directly or indirectly, and not in any way to assist, encourage, or induce any State, group of States, or international organizations to manufacture or otherwise acquire any of the agents, toxins, weapons, equipment or means of delivery.
* In accordance with its constitutional processes, take any necessary measures to prohibit and prevent the development, production, stockpiling, acquisition, or retention of the agents, toxins, weapons, equipment and means of delivery, within the territory of such State, under its jurisdiction or under its control anywhere.

In fulfillment of the provision requiring measures to prohibit the development, etc. of agents, toxins, etc., the United States passed the Anti-Terrorism and Effective Death Penalty Act of 1996.[176] Pursuant to this act the Centers for Disease Control established a list of biological agents and toxins requiring special controls on their use and distribution for any purposes (peaceful or otherwise).[177] This list is reproduced in Table L-3. Facilities using these agents must keep records of their consumption and disposal. Any transmission of these agents can only occur between facilities authorized by the Centers for Disease Control and records of transmission must be kept.

In the international arena, the primary shortcomings of the BTWC are the lack of effective verification protocols and the lack of provision for enforcement (sanctions for violation). Possible improvements to the Convention are discussed in Reference 178.

Table L-3. Agents controlled under U.S. laws. [176,177]

VIRUSES

- Crimean-Congo hemorrhagic fever virus
- Eastern Equine Encephalitis virus
- Ebola viruses
- Equine Morbillivirus
- Lassa fever virus
- Marburg virus
- Rift Valley fever virus
- South American hemorrhagic fever viruses (Junin, Machupo, Sabia, Flexal, Guanarito)
- Tick-borne encephalitis complex viruses
- Variola major virus (Smallpox virus)
- Venezuelan Equine Encephalitis virus
- Yellow fever virus
- **EXEMPTIONS:** Vaccine strains of viral agents

BACTERIA

- *Bacillus anthracis*
- *Brucella abortus, B. melitensis, B. suis*
- *Burkholderia (Pseudomonas) mallei*
- *Burkholderia (Pseudomonas) pseudomallei*
- *Clostridium botulinum*
- *Francisella tularensis*
- *Yersinia pestis*
- **EXEMPTIONS:** Vaccine strains

RICKETTSIAE

- *Coxiella burnetii*
- *Rickettsia prowazekii*
- *Rickettsia rickettsii*

FUNGI

- *Coccidioides immitis*

TOXINS

- Abrin
- Aflatoxins
- Botulinum toxins
- *Clostridium perfringens* epsilon toxin
- Conotoxins
- Diacetoxyscirpenol
- Ricin
- Saxitoxin
- Shigatoxin
- Staphylococcal enterotoxins
- Tetrodotoxin
- T-2 toxin
- **EXEMPTIONS: -** Toxins for medical use
  - Toxins inactivated for use as vaccines

RECOMBINANT ORGANISMS/MOLECULES

- Genetically modified microorganisms or genetic elements from organisms above, shown to encode for a factor associated with a disease
- Genetically modified microorganisms or genetic elements that contain nucleic acid sequences coding for any of the toxins above, or their toxic subunits

Non-Proliferation Treaty and IAEA Safeguards

The **Non-Proliferation Treaty** (or NPT) is the primary international agreement for limiting the spread of nuclear weapons. Formally titled the ***"Treaty on the Non-Proliferation of Nuclear Weapons"***, the NPT was [179]:

* Signed on 1 July 1968 by the United States, United Kingdom, Soviet Union, and many other states
* Ratified by the U. S. President on 24 November 1969
* Treaty entered into force on 5 March 1970

Countries of special note that have ratified or acceded to the NPT include:

France	China
South Africa	North Korea
Algeria	Iran
Iraq	Argentina
Japan	Taiwan
Republic of Korea	Libya

Countries of special note that have not signed or acceded to the NPT include:

India	Pakistan
Israel	Syria

The nuclear-weapons holding states of the former Soviet Union are a special case. The Russian Federation has formally declared that it will uphold all rights and responsibilities of the Soviet Union with respect to this treaty (as a nuclear weapons-possessing state). Belarus, Kazakhstan, and Ukraine have all filed letters of accession to the treaty as non-nuclear weapon states and have transferred all of their nuclear weapons to the control of the Russian Federation. The Lisbon Protocol [180] to the Strategic Arms Reduction Treaty (START) formally documented the succession of these four states to the responsibilities of the former Soviet Union, not only with respect to START, but also explicitly with respect to the NPT.

Under the NPT, signatory states are divided into nuclear-weapon states and non-nuclear-weapon states with different responsibilities: **nuclear-weapon states** (possessing nuclear weapons and/or the capability to manufacture nuclear weapons) and **non-nuclear-weapon states** (lacking nuclear weapons and the capability to manufacture nuclear weapons). The capability to manufacture nuclear weapons means possession of weapons-grade fissionable materials or facilities capable of producing highly-enriched uranium or of separating plutonium from irradiated nuclear fuel, possession of nuclear weapons designs, and control of facilities for translating those designs into hardware. A country which has built all of the parts, but not yet assembled them into a nuclear explosive device, is assumed to possess nuclear weapons. In the provisions listed below, "**source material**" is uranium or thorium metal, or their ores. "**Special fissionable material**" is Uranium-233, Plutonium (all isotopes), and enriched Uranium-235.

The principal provisions of the NPT include:

Nuclear-weapon states will not:

* transfer nuclear weapons to any other state.
* give control of nuclear weapons to any other state.
* assist, encourage, or induce non-nuclear-weapon states to acquire nuclear weapons or control over nuclear weapons.

Non-nuclear-weapon states will not:
* receive nuclear weapons from any state.
* accept control over nuclear weapons from any state.
* attempt to acquire nuclear weapons or control over nuclear weapons.

Non-nuclear-weapon states will:
* accept safeguards to prevent diversion of nuclear energy from peaceful purposes to nuclear weapons.
* conclude a safeguards agreement with the International Atomic Energy Agency (IAEA) in accordance with the IAEA safeguards program.

All states will not:
* provide source or special fissionable material to any party unless that material is subject to an IAEA safeguards program.
* provide equipment or material designed for processing, use, or production of special fissionable material unless the source or special fissionable material is subject to an IAEA safeguards program.

The treaty shall not affect the inalienable right of all states to pursue peaceful uses of nuclear energy.

The NPT has been reasonably effective in preventing proliferation of nuclear weapons. The primary reason for this is the ability to apply sanctions to non-complying states. The weakness is that all of these sanctions apply to the IAEA Safeguard requirement (see the section of this chapter that deals with IAEA Safeguards). States that violate the NPT are prevented from legally acquiring fissionable materials. If the violator has a nuclear power program, sanctions on obtaining nuclear fuel could be catastrophic. The weakness is that a violator might possess sufficient indigenous uranium ore and an enrichment capability that would negate any need to obtain fuel from outside sources. Alternatively, the violator might possess some item of commerce sufficiently attractive to tempt an non-NPT state with uranium enrichment capability to sell to the violator or to tempt an NPT state to violate the agreement. Uranium has always been available if the price is high enough. Sanctions that affected other areas of a proliferator's economy might have more effect.

The NPT called for a conference of the States Parties after 25 years to determine if the Treaty warranted cancellation, extension for an additional fixed period, or extension for an indefinite period. This conference was held in 1995 and the participants voted to extend the NPT indefinitely. [181]

The signatories of the Non-Proliferation Treaty have chosen to control the proliferation of nuclear weapons by the applications of "safeguards" on production of, access to, and transfer of fissionable material. The safeguards are such that the reasonable development of peaceful applications of nuclear energy is not unnecessarily hindered. The International Atomic Energy Agency (IAEA) is the organization that has been selected to supervise and implement the safeguards process. The Non-Proliferation Treaty specifies that the mechanism for control of proliferation will be Safeguards agreements negotiated between the individual states and the IAEA.

Safeguards agreements are described in **"*The Structure and Content of Agreements Between the Agency and States Required in Connection with the Treaty on the Non-Proliferation***

of Nuclear Weapons", IAEA Information Circular INFCIRC/153 (Corrected) (June 1972).[182] The Safeguards Agreement between the United States and the IAEA may be found in Reference [183]. A Safeguards Agreement consists of two parts.

Part I of the Safeguards Agreement should (among other things):

* Contain an undertaking by the State to accept safeguards on all source or fissionable material in all peaceful nuclear activities under its control for the purpose of verifying that such material is not diverted to nuclear weapons or nuclear explosive devices.
* Provide for the IAEA's right and obligation to ensure that safeguards will be applied on all source or special fissionable material in all peaceful nuclear activities under the State's control.
* Provide that the IAEA and the State shall cooperate to facilitate the implementation of the safeguards.
* Provide that safeguards shall be implemented in a manner designed to:
    - avoid hampering the economic and technological development of the State in the field of peaceful nuclear activities
    - avoid undue interference in the State's peaceful nuclear activities
    - be consistent with prudent management practices required for the economic and safe conduct of nuclear activities
* Provide that the IAEA shall take every precaution to protect commercial and industrial secrets.
* Provide that in implementing safeguards the IAEA shall take full account of technological developments in the fields of safeguards and shall ensure optimum cost-effectiveness. Cost-effectiveness shall include concentrating the verification procedures on those stages of the nuclear fuel cycle involving nuclear material from which nuclear weapons could be readily made.
* Provide that the State shall establish and maintain a system of accounting for and control of all nuclear material subject to safeguards.
* Provide that the IAEA shall be given information concerning nuclear material subject to safeguards and the features of facilities relevant to safeguarding such material.
* Provide that the State shall ensure that IAEA inspectors can effectively discharge their functions.
* If the State is a Nuclear Weapons State, provide that materials and facilities used in nuclear weapons activities shall not be subject to safeguards until such time as that material or facilities are converted to peaceful applications.

Part II of the Safeguards Agreement should specify the procedures to be applied for the implementation of the safeguards provisions of Part I. Specifically, the Agreement should:

* Provide that the objective of safeguards is the timely detection of diversion of significant quantities of nuclear material from peaceful nuclear activities to the manufacture of nuclear weapons and deterrence of such diversion by the risk of early detection.
* Provide for the use of material accountancy as a safeguards measure of fundamental importance, with containment and surveillance as important complementary measures.
* Provide that the technical conclusion of the Agency's verification activities shall be a statement, in respect of each material balance area, of the amount of material un-

accounted for over a specific period, giving the limits of accuracy of the amounts stated.

* Provide that the IAEA shall make full use of the State's system of accounting for and control of all nuclear material.
* Provide that the accounting system shall be based on **material balance areas**.
* Provide that safeguards begin when any nuclear material is imported, exported, or converted to a composition and purity suitable for fuel fabrication or isotopic enrichment.
* Provide that design information of nuclear facilities be provided to the IAEA by the State.
* Provide that records are kept in respect of each material balance area as part of a national system of accounting for nuclear material.
* Provide that the State shall provide reports to the IAEA describing the inventory of nuclear material and changes in that inventory.
* Provide that the IAEA shall have the right to make inspections to verify the information in any reports or documents submitted by the State.
* Provide that any potential transfers of nuclear material between States shall be described in advance to the IAEA.

The Safeguards System is described in **"*The Agency's Safeguards System*"** IAEA Information Circular INFCIRC/66/Rev.2 (16 September 1968).[184] Safeguards will only be implemented if there exists a Safeguards Agreement negotiated between the State and the IAEA. Nuclear material shall be subject to IAEA Safeguards if:

* The material was submitted to safeguards under a Safeguards Agreement.
* The material was produced, processed, or used in a principal nuclear facility subject to a Safeguards Agreement.
* The material was produced in or by the use of material subject to a Safeguards Agreement.

Principal nuclear facilities include reactors, plants for processing nuclear materials irradiated in a reactor, plants for separating the isotopes of nuclear materials, or plants for processing or fabricating nuclear materials.

Small amounts of nuclear material may be exempted from safeguards upon request. The exempted material may not exceed:

* 1 kilogram in total of special fissionable material, consisting of one or more of:
  - plutonium
  - uranium with enrichment of 20% or higher, determined by the material weight times the enrichment
  - uranium with enrichment less than 20% but greater than natural uranium, determined by the material weight times five times the square of its enrichment.
* 10 metric tons in total of natural uranium and depleted uranium with an enrichment greater than 0.5%.
* 20 metric tons of depleted uranium with enrichment of 0.5% or less.
* 20 metric tons of thorium.

Produced or used nuclear material shall be exempted if it is:

* plutonium produced in the fuel of a reactor whose production rate is less than 100 g(Pu)/yr.

* produced in a reactor with maximum calculated continuous power less than 3 thermal megawatts. Integrated thermal power of exempted reactors may not exceed 6 thermal megawatts.

The following procedures shall be followed in implementing the Safeguards System. The Agency shall **review the design of principal nuclear facilities** to determine that a facility will permit the effective application of safeguards. The review shall occur as early as possible using information supplied by the State.

The State shall arrange for the **keeping of records** with respect to principal nuclear facilities and with respect to all safeguarded nuclear material outside such facilities. The records shall consist of accounting records of all safeguarded nuclear material and operating records for principal nuclear facilities. Records shall be kept for at least two years.

The State shall submit to the IAEA **reports with respect to the production, processing, and use of safeguarded nuclear material** in or outside principal nuclear facilities. Timing and number of such reports will be negotiated. Reports need only include such information as is relevant to the purpose of safeguards. Routine reports include accounting reports and operating reports. Routine reports should show the receipt, transfer out, inventory, and use of all safeguarded nuclear material. In principle, these reports would account for all nuclear material coming into, residing in, and going out of a facility (or a material balance area). Net input minus net output would be expected to equal material remaining in the area plus "losses". Losses might include airborne dust or machining wastes, chemically altered material deposited as corrosion in piping, leakage from storage tanks, material lost due to radioactive decay or fission (in reactors), material that is unrecoverable from processing solvents, and material consumed in testing and quality control. Every attempt is made to calculate such losses, but accuracy is difficult. In practice, in a plant with a large throughput, it may not be possible to balance the accounts to an accuracy any better than 250 kg of nuclear material.[185] Unfortunately, this is enough to make at least twenty-five ten nuclear weapons. Operating reports should show the use made of each principal nuclear facility since the last report and the planned program of future use until the next report. The State shall submit special reports to the IAEA if any unusual incident occurs involving actual or potential loss or destruction of, or damage to any safeguarded nuclear material or principal nuclear facility; or if there is good reason to believe that safeguarded nuclear material is lost or unaccounted for in quantities that exceed the normal operating and handling losses that have been accepted by the IAEA as characteristic of the facility. If the IAEA requests it, the State shall submit amplifications or clarifications of any report. Reports for nuclear reactors shall be provided at least twice a year, but in no case more than 12 per year.

The IAEA may **inspect safeguarded nuclear materials and principal nuclear facilities**. The purpose of safeguards shall be to verify compliance with Safeguards Agreements. The number, duration, and intensity of such inspections shall be kept to the minimum consistent with the effective implementation of safeguards. Inspectors shall neither operate any facility themselves nor direct the staff to carry out any particular operation. Routine inspections may include:

* Audit of records and reports
* Verification of the amount of safeguarded material by physical inspection, measurement, and sampling

* Examination of principal nuclear facilities, including a check of their measuring instruments and operating characteristics
* Checking the operations carried out at principal nuclear facilities and at research and development facilities containing safeguarded nuclear material.

The IAEA may carry out special inspections if any circumstance indicates that such inspection is desirable. The IAEA may also inspect any substantial amount of nuclear material that is to be transferred outside the jurisdiction of a State. Reactors are subject to one inspection per year for every 5 kg of nuclear material that they have in inventory, have as annual throughput, or have a maximum annual potential production. If any of these exceeds 60 kg per year, then the IAEA shall have continuous access to the facility. Inspections of other facilities will be subject to the same inspection rate limitation.

Storage facilities for nuclear material shall have their designs reviewed by the IAEA. The method and procedure for sealing the facility shall be mutually agreed upon by the State and the IAEA. Accounting reports for material in sealed storage shall be submitted twice per year. One routine inspection of sealed material may be conducted annually. Removal of material from sealed storage requires advance notification of the IAEA.

Since the latter years of the 20th Century, the IAEA has been attempting to strengthen the Safeguards process by including more of the nuclear fuel cycle in the records and reporting process. The IAEA formulated the "Model Protocol Additional to the Agreement(s) Between State(s) and the International Atomic Energy Agency for the Application of Safeguards" INFCIRC/540 (Corrected) (September 1997) [186] and requested that all States with existing Safeguards agreements also sign the Protocol (or a negotiated version thereof). As of early 2000, roughly 50 signatory States had also signed the Protocol, including the United States.

The principal provisions of the Protocol include that the State Party shall provide information on and access to specific activities related to the nuclear fuel cycle. Specific information shall include:

* A general description of and information specifying the location of nuclear fuel cycle-related research and development activities not involving nuclear materials.
* Information identified by the IAEA on the basis of expected gains in effectiveness on operational facilities and at locations outside facilities where nuclear material is customarily used.
* A general description of each building on each site, including its use and its contents.
* A description of the scale of operations for each location engaged in any of the activities specified in Annex I.
* Information specifying the location, operational status and the estimated annual production capacity of all uranium mines, uranium concentration plants, and thorium concentration plants.
* Information regarding source material which has not reached the composition and purity suitable for fuel fabrication or for being isotopically enriched.
* Information regarding the quantities, uses, and locations of nuclear material exempted from safeguards.
* Information regarding the location or further processing of intermediate or high-level waste containing plutonium, high enriched uranium, or uranium-233 on which

safeguards have been terminated.
* Information regarding the export and/or import of equipment or non-nuclear material specified in Annex II.

Access shall also be provided to any materials, facilities, or sites identified in any of the above, for purposes of verifying that nuclear material is not being diverted or that preparations are not being made for the future diversion of nuclear materials.

The following activities are listed in Annex I and whose details must be reported in accordance with Article 2.a.(iv) of the Protocol.

* The manufacture of centrifuge rotor tubes or the assembly of gas centrifuges.
* The manufacture of diffusion barriers.
* The manufacture or assembly of laser-based [isotope separation] systems.
* The manufacture or assembly of electromagnetic isotope separators.
* The manufacture or assembly of columns or extraction equipment [for isotopically enriching, separating, or purifying nuclear materials]
* The manufacture of aerodynamic separation nozzles or vortex tubes.
* The manufacture or assembly of uranium plasma generation systems.
* The manufacture of zirconium tubes.
* The manufacture or upgrading of heavy water or deuterium.
* The manufacture of nuclear grade graphite.
* The manufacture of flasks [for the transportation and/or storage] of irradiated fuel.
* The manufacture of reactor control rods.
* The manufacture of criticality safe tanks and vessels.
* The manufacture of irradiated fuel element chopping machines.
* The construction of hot cells.

The following equipment and non-nuclear material is listed in Annex II and whose export or import must be reported in accordance with Article 2.a.(ix) of the Protocol.

1. Reactors and equipment therefor
   - 1.1 Complete nuclear reactors
   - 1.2 Reactor pressure vessels
   - 1.3 Reactor fuel charging and discharging machines
   - 1.4 Reactor control rods
   - 1.5 Reactor pressure tubes
   - 1.6 Zirconium tubes
   - 1.7 Primary coolant pumps
2. Non-nuclear materials for reactors
   - 2.1 Deuterium and heavy water
   - 2.2 Nuclear grade graphite
3. Plants for the reprocessing of irradiated fuel elements, and equipment especially designed or prepared therefor
   - 3.1 Irradiated fuel element chopping machines
   - 3.2 Dissolvers
   - 3.3 Solvent extractors and solvent extraction equipment
   - 3.4 Chemical holding or storage vessels
   - 3.5 Plutonium nitrate to oxide conversion system

3.6 Plutonium oxide to metal production system

4. Plants for fabrication of fuel elements
5. Plants for separation of isotopes or uranium and equipment, other than analytical instruments, especially designed or prepared therefor
    - 5.1 Gas centrifuges and assemblies and components especially designed or prepared for use in gas centrifuges
    - 5.2 Especially designed or prepared auxiliary systems, equipment and components for gas centrifuge enrichment plants
    - 5.3 Especially designed or prepared assemblies and components for use in gaseous diffusion equipment
    - 5.4 Especially designed or prepared auxiliary systems, equipment and components for use in gaseous diffusion enrichment
    - 5.5 Especially designed or prepared systems, equipment and components for use in aerodynamic enrichment plants
    - 5.6 Especially designed or prepared systems, equipment and components for use in chemical exchange or ion exchange enrichment plants
    - 5.7 Especially designed or prepared systems, equipment and components for use in laser-based enrichment plants
    - 5.8 Especially designed or prepared systems, equipment and components for use in plasma separation enrichment plants
    - 5.9 Especially designed or prepared systems, equipment and components for use in electromagnetic enrichment plants

6 Plants for the production of heavy water, deuterium and deuterium compounds and equipment especially designed or prepared therefor
    - 6.1 Water-hydrogen sulfide exchange towers
    - 6.2 Blowers and compressors
    - 6.3 Ammonia-hydrogen exchange towers
    - 6.4 Tower internals and stage pumps
    - 6.5 Ammonia crackers
    - 6.6 Infrared absorption analyzers
    - 6.7 Catalytic burners

7 Plants for the conversion or uranium and equipment especially designed or prepared therefor
    - 7.1 Especially designed or prepared systems for the conversion of uranium ore concentrates to UO_3
    - 7.2 Especially designed or prepared systems for the conversion of UO_3 to UF_6
    - 7.3 Especially designed or prepared systems for the conversion of UO_3 to UO_2
    - 7.4 Especially designed or prepared systems for the conversion of UO_2 to UF_4
    - 7.5 Especially designed or prepared systems for the conversion of UF_4 to UF_6
    - 7.6 Especially designed or prepared systems for the conversion of UF_4 to U metal
    - 7.7 Especially designed or prepared systems for the conversion of UF_6 to UO_2
    - 7.8 Especially designed or prepared systems for the conversion of UF_6 to UF_4

The **objective of safeguards** is the **timely detection of diversion** of significant quantities of nuclear material from peaceful nuclear activities to the manufacture of nuclear weapons and **deterrence of such diversion by the risk of early detection**. The Safeguards System was designed to deter the continuing diversion of small amounts of material by the State or by individuals or groups associated with the nuclear industry. Inadequate attention is paid to the prevention of theft or related diversion of larger amounts of materials. Seals are the only form of physical security even mentioned in the description of the Safeguards System. Containment (physical barriers to material movement) and surveillance (e.g., cameras with recorders and recorders attached to measurement devices) are acknowledged as complementary measures to material accounting in the Safeguards Agreement document but not in the Safeguards description. It is a certainty that some degree of containment and surveillance is applied to all principal nuclear facilities. Nevertheless, a risk that material may be discovered to be missing after passage of a few days, weeks, or months is no deterrence to a criminal group or organization. It is only a deterrence to the State Government or individuals desiring continued association with the nuclear industry. The risk of theft is particularly strong when material is shipped between states.

To address this deficiency a convention was negotiated between the signatories to the Non-Proliferation Treaty to provide for the physical protection of nuclear material at all times whether in transit, use or storage. Formally titled the **"*Convention on the Physical Protection of Nuclear Material*"**, the **Nuclear Material Convention** was: [187]

* Signed on 3 March 1980 by the United States and several other countries
* Ratified by the U. S. President on 4 September 1981
* Convention entered into force on 8 February 1987

The principle provisions of the Nuclear Materials Convention include:
Each State Party shall:

* Take appropriate steps within the framework of its national law and consistent with international law to ensure that during international transport, nuclear material within its territory or on board a ship or aircraft under its jurisdiction is protected at the levels described in Annex I.
* Not export (or import) or authorize the export (or import) of nuclear material unless it has received assurances that the material will be protected under international transport at the levels in Annex I.
* Not allow the transit of its territory by land or internal waterways or through its airports or seaports of nuclear material between States that are not party to this convention unless the State has received assurance that this material will be protected during international transport at the levels described in Annex I.
* In the case of theft, robbery, or any other unlawful taking of nuclear material or credible threat thereof, in accordance with their national law, provide cooperation and assistance to the maximum extent feasible in the recovery and protection of such material to any State that so requests.
* Enact legislation that makes any of the following a punishable offense under its national law:
    - unauthorized receipt, possession, use, transfer, alteration, disposal, or dispersal of nuclear material, and which causes or is likely to cause death or serious injury to any person or substantial damage to property.
    - theft or robbery of nuclear material
    - embezzlement or fraudulent obtaining of nuclear material
    - an act constituting a demand for nuclear material by threat or use of force or by any other means of intimidation
    - a threat to use nuclear material to cause death or serious injury to any person or

substantial property damage
- a threat to commit theft or robbery of nuclear material in order to compel any person, organization, or State to do or to refrain from doing any act.
- any attempt to commit any of the above acts.

* Make the offenses described above punishable by appropriate penalties which take into account their grave nature.

In the context of this Convention, nuclear material means: plutonium (except material in which the concentration of the isotope Pu-238 exceeds 80%), uranium-233, uranium enriched in the isotopes U-233 or U-235 or both, natural uranium in any form other than ore or ore-residue, or any material containing one or more of the foregoing materials. This Convention shall apply to nuclear material used for peaceful purposes while in international transport, as well to nuclear material used for peaceful purposes while in domestic use, storage, and transport.

Annex II categorizes nuclear materials for the purposes of the level of protection needed. Category I materials include:

* 2 kg or greater of plutonium
* 5 kg or greater of U-235 enriched to 20% or higher
* 2 kg or greater of U-233

Category II materials include:

* 500 to 2000 g of plutonium
* 1 to 5 kg of U-235 enriched to 20% or higher
* 10 kg or greater of U-235 enriched to levels between 10% and 20%
* 500 to 2000 g of U-233
* Depleted or natural uranium, thorium or low enriched fuel, plutonium, U-233, or U-235 if previously irradiated in a nuclear reactor and currently possessing a radiation level exceeding 100 rads/hr at one meter unshielded.

Category III materials include:

* 15 to 500 g of plutonium
* 15 to 1000 g of U-235 enriched to 20% or higher
* 1 to 10 kg of U-235 enriched to levels between 10% and 20%
* 10 kg or greater of U-235 enriched above natural levels but less than 10%
* 15 to 1000 g of U-233.

Quantities below Category III levels and natural uranium should be protected in accordance with prudent management practices.

Annex I provides for the following degrees of protection:

<u>Storage</u>	Category III	Storage within an area to which access is controlled.
	Category II	Storage within an area under constant surveillance by guards or electronic devices, surrounded by a physical barrier with a limited number of entry points under appropriate control.
	Category I	Storage within an area as defined for Category II, to which in addition, access is restricted to persons whose trustworthiness has been determined and which is under surveillance by guards who are in close communication with appropriate response forces. Specific measures should have as their object, the detection and prevention

		of any assault, unauthorized access or unauthorized removal of material.
Transport	Category III Category II	Transportation shall take place under special precautions including prior arrangements among sender, receiver, and carrier, and prior agreement between persons subject to the jurisdiction and regulation of exporting and importing States, specifying time, place, and procedures for transferring transport responsibility.
	Category I	Transportation shall take place under special precautions above, and in addition, under constant surveillance by escorts and under conditions which assure close communication with appropriate response forces.

Transport of natural uranium other than ore in quantities exceeding 500 kg shall include advance notification of shipment specifying mode of transport, expected time of arrival, and confirmation of receipt of shipment.

Taken together, Safeguards and the Nuclear Material Convention provide reasonable protection for nuclear materials. However, we have seen that the undetected diversion of small but substantial amounts may be possible in some nuclear facilities. A State has other options for clandestine acquisition of nuclear materials that can bypass the Safeguards System. These are discussed in detail in Reference [188]. Although they are not perfect, no state that has accepted Safeguards controls has developed nuclear weapons while the Safeguards were in force.

Nuclear Test Ban Treaties

A series of treaties has been negotiated governing the conduct of nuclear weapons tests. In sequence, these prohibited first atmospheric tests, outer space test, and underwater tests; then any test exceeding 150 kT in yield; and finally any and all nuclear explosions. The first of these treaties was the Limited Test Ban Treaty.

Limited Test Ban Treaty – Formally titled the ***"Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water"***, the Limited Test Ban Treaty (LTBT) was [189]:

* Signed on 5 August 1963 by the United States, United Kingdom, Soviet Union, and many other states
* Ratification was advised by the U. S. Senate on 24 September 1963
* Ratified by the U. S. President on 10 October 1963
* Ratification document was deposited on 10 October 1963
* Treaty entered into force on 10 October 1963

Countries of special note which have ratified or acceded to the LTBT include:

Argentina	Australia	Belarus
Brazil	Canada	Egypt
Germany	India	Indonesia
Iran	Iraq	Israel
Japan	Republic of Korea	Libya
Mexico	Pakistan	Russian Federation(USSR)
South Africa	Syria	Taiwan
Ukraine	United Kingdom	United States

Countries which have signed but not ratified the LTBT include:

Algeria	Burkina Faso	Burundi
Cameroon	Ethiopia	Haiti
Mali	Paraguay	Portugal
Somalia		

Countries of special note which have neither signed nor acceded to the LTBT include:

China	Cuba	France
North Korea	Vietnam	

The principal provisions of the LTBT include:

Parties to this treaty undertake to:

* Prohibit, prevent, and not to carry out any nuclear weapon test explosion or any other nuclear explosion, at any place under their jurisdiction or control:
  - in the atmosphere
  - in outer space
  - under water, including territorial waters or high seas
  - in any other environment if such explosion causes radioactive debris to be present outside the territorial limits of the state under whose jurisdiction or control such explosion is conducted
* Refrain from causing, encouraging, or in any way participating in the carrying out of any nuclear weapon test explosion or any other nuclear explosion in any of the

environments above or which would have the effect described above.

Threshold Test Ban Treaty – Formally titled the "***Treaty Between the United States of America and the Union of Socialist Republics on the Limitation of Underground Nuclear Weapon Tests***", the Threshold Test Ban Treaty (TTBT) was [190]:

* Signed on 3 July 1974 by the United States and the Soviet Union
* Ratified by the U. S. President on 8 December 1990
* Treaty entered into force on 11 December 1990

The principal provisions of the TTBT include:
Parties to this treaty undertake to prohibit, prevent, and not to carry out any underground nuclear weapon test having a yield exceeding 150 kilotons.

Peaceful Nuclear Explosions Treaty – Formally titled the "***Treaty Between the United States of America and the Union of Socialist Republics on Underground Nuclear Explosions for Peaceful Purposes***", the Peaceful Nuclear Explosions (PNE) Treaty was [191]:

* Signed on 28 May 1976 by the United States and the Soviet Union
* Ratified by the U. S. President on 8 December 1990
* Treaty entered into force on 11 December 1990

The principal provisions of the PNE treaty include:
Parties to this treaty undertake to prohibit, prevent, and not to carry out:

* Any individual nuclear explosion (including those for peaceful purposes) having a yield exceeding 150 kT
* Any group explosion (including those for peaceful purposes) having an aggregate yield exceeding 150 kT unless each individual explosion can be identified and the aggregate yield is less than 1500 kT.

Comprehensive Test Ban Treaty – Formally titled "***The Comprehensive Test Ban Treaty***", the CTBT was [24]:

* Signed on 24 September 1996 by the United States, Russian Federation, France, United Kingdom, China, Israel, and many other states
* Ratification was is awaiting the advice and consent of the U. S. Senate (ratification is in doubt until such time as the stability and reliability of the stockpile of existing weapons can be adequately assured without occasional full-scale testing)
* Treaty has not entered into force pending many outstanding ratifications (countries whose names appear in bold type in the list of signatories must ratify the treaty before it can enter into force)

Countries of note that have signed and ratified the CTBT include:

Australia	**Argentina**	**Austria**
Bangladesh	**Belgium**	**Brazil**
Bulgaria	**Canada**	**Colombia**
Egypt	**Finland**	**France**
Germany	**Hungary**	**Italy**
Japan	**Mexico**	**Netherlands**
Norway	**Peru**	**Poland**

Republic of Korea	**Romania**	**Russian Federation**
Slovakia	**South Africa**	**Spain**
Sweden	**Switzerland**	**Turkey**
Ukraine	**United Kingdom**	

Countries that have signed but not yet ratified the CTBT include:

Algeria	Belarus	**Chile**
China	**Indonesia**	**Iran**
Israel	Kazakhstan	**United States**
Vietnam		

Countries of special note that have not signed the CTBT include:

India	Iraq	Libya
North Korea	**Pakistan**	Syria
Taiwan (not allowed to sign due to PRC)		

The principal provisions of the CTBT include:

Each state party undertakes:

* not to carry out any nuclear weapon test explosion or any other nuclear explosion, and to prohibit and prevent any such nuclear explosion at any place under its jurisdiction or control.
* to refrain from causing, encouraging, or in any way participating in the carrying out of any nuclear weapon test explosion or any other nuclear explosion.

The parties will establish the Comprehensive Nuclear Test-Ban Organization to ensure the implementation of the provisions of this treaty, including those for international verification of compliance.

Nuclear-Free Zones and Other Nuclear Non-Proliferation Agreements

Several geographically related groups of nations have undertaken to ban nuclear weapons not only from their individual countries but from an entire geographical region. They established several "nuclear free zones" within which nuclear weapons are absolutely prohibited. Note that such treaties cannot have jurisdiction over ships navigating in international waters. The treaties creating these zones are described below.

Treaty of Tlatelolco – Formally titled the **"*Treaty for the Prohibition of Nuclear Weapons in Latin America*"**, the Treaty of Tlatelolco was [192]:

* Signed 14 Feb 1967
* Treaty entered into force 22 Apr 1968

Virtually all countries in Latin and South America have signed and ratified the Treaty of Tlatelolco except:

Argentina	Belize
Dominica	St. Lucia

The following countries have signed and ratified Protocol I to the Treaty of Tlatelolco:

France	Netherlands
United Kingdom	United States

The following nuclear weapons states have signed and ratified Protocol II to the Treaty of Tlatelolco:

China	France
Union of Soviet Socialist Republics	United Kingdom
United States	

The principal provisions of the Treaty of Tlatelolco include:

The contracting parties undertake to:

* Use exclusively for peaceful purposes the nuclear material and facilities which are under their jurisdiction, and to prohibit and prevent in their respective territories;
  (a) the testing, use, manufacture, production, or acquisition by any means whatsoever of any nuclear weapons, by the parties themselves, directly or indirectly, on behalf of anyone else or in any other way; and

(b) the receipt, storage, installation, deployment, and any form of possession of any nuclear weapons, directly or indirectly, by the parties themselves, by anyone on their behalf or in any other way.

* Refrain from engaging in, encouraging or authorizing, directly or indirectly, or in any way participating in the testing, use, manufacture, production, possession, or control of any nuclear weapon.

Protocol I calls on nations outside the Treaty zone to apply the denuclearization provisions of the Treaty to the territories in the zone for which they are *de jure* or *de facto* responsible. Protocol II calls on nuclear weapons states to respect the denuclearized status of the zone, not to contribute to acts involving violation of obligations of the parties to the Treaty, and not to use or threaten to use nuclear weapons against the contracting parties. The treaty does not prohibit the use of peaceful nuclear explosives provided that those explosives cannot be used for any military purpose. In practice it is almost impossible to guarantee that a nuclear explosive is incapable of military utility.

The United States is responsible for Puerto Rico, the Virgin Islands, and the naval base at Guantanamo Bay, Cuba under Protocol I of the treaty. The United States has agreed to abide by Protocol I to the treaty. This means that we may not store, manufacture any part of, test, or use nuclear weapons in these territories.

Treaty of Rarotonga – Formally titled the **"*South Pacific Nuclear Free Zone Treaty*"**, the Treaty of Rarotonga was [193]:

* Signed 6 Aug 1985

* Treaty entered into force 11 Dec 1986

The following countries have signed and ratified the Treaty of Rarotonga:

Australia	Cook Islands
Fiji	Kiribati
Nauru	New Zealand
Niue	Papua New Guinea
Solomon Islands	Tonga
Tuvalu	Vanuatu
Western Samoa	

The principal provisions of the Treaty of Rarotonga include:

Each party undertakes:

* Not to manufacture or otherwise acquire, possess or have control over any nuclear explosive device by any means anywhere inside or outside the South Pacific Nuclear Free Zone.

* Not to seek or receive any assistance in the manufacture or acquisition of any nuclear explosive device.

* Not to provide source or special fissionable material, or equipment or material especially designed or prepared for the processing, use or production of special fissionable material for peaceful purposes to any state unless subject to IAEA safeguards.

* To support the continued effectiveness of the international non-proliferation system based on the NPT and the IAEA safeguards system.

* To prevent the stationing of any nuclear explosive device in its territory.

* To prevent in its territory the testing of any nuclear explosive device.
* Not to dump radioactive wastes or other radioactive matter at sea anywhere within the South Pacific Nuclear Free Zone.
* To prevent the dumping of radioactive wastes and other radioactive matter by anyone in its territorial sea.

The South Pacific Nuclear Free Zone is defined by the area bounded by a line defined by precise geographic locations specified in the treaty (and essentially encompassing all of the Territories of the signatories, most of the South Pacific Ocean, and many non-signatory entities such as New Caledonia, French Polynesia, American Samoa, and numerous other small islands controlled by the United States, United Kingdom, or France).

The Treaty permits each party to exercise its sovereign rights and to remain free to decide for itself whether to allow visits by foreign ships and aircraft to its ports and airfields, transit of its airspace by foreign aircraft, and navigation by foreign ships in its territorial sea or archipelagic waters in a manner not covered by the rights of innocent passage, archipelagic sea lane passage, or transit passage of straits.

Treaty of Pelindaba – Formally titled "***The African Nuclear-Weapon-Free Zone Treaty***", the Treaty of Pelindaba was [194]:

* Signed 11 Apr 1996
* The treaty's entry into force awaits sufficient ratifications.

Countries which have signed and ratified the Treaty of Pelindaba include (as of 19 Nov. 1998):

Algeria	Burkina Faso	Gambia
Mauritania	Mauritius	South Africa
Tanzania	Zimbabwe	

Countries which have signed but not yet ratified the Treaty include:

Angola	Benin	Botswana
Burundi	Cameroon	Cape Verde
Central African Republic	Chad	Comoros
Congo	Cote d'Ivoire	Dem. Rep. of Congo
Djibouti	Egypt	Eritrea
Ethiopia	Gabon	Ghana
Guinea	Guinea-Bissau	Kenya
Lesotho	Liberia	Libya
Malawi	Mali	Morocco
Mozambique	Namibia	Niger
Nigeria	Rwanda	Sao Tome & Principe
Senegal	Seychelles	Sierra Leone
Sudan	Swaziland	Togo
Tunisia	Uganda	Zambia

The following countries have not signed the Treaty:

Equatorial Guinea	Madagascar	Somalia

The following countries have signed (* denotes ratified as well) Protocol I to the Treaty:

*China	*France	Russian Federation
United Kingdom	United States of America	

The following countries have signed (* denotes ratified as well) Protocol II to the Treaty:

*China	*France	Russian Federation
United Kingdom	United States of America	

France has signed and ratified Protocol III. Spain has neither signed nor ratified Protocol III.

The principle provisions of the treaty include:
Each party undertakes:

* Not to conduct research on, develop, manufacture, stockpile or otherwise acquire, possess or have control over any nuclear explosive device by any means anywhere.
* To prohibit, in its territory, the stationing of any nuclear explosive device.
* Not to test any nuclear explosive device.
* To prohibit in its territory the testing of any nuclear explosive device.
* To declare any capability for the manufacture of nuclear explosive devices.
* To dismantle and destroy any nuclear explosive device that it has manufactured prior to the coming into force of this treaty.
* To destroy facilities for the manufacture of nuclear explosive devices, or where possible, to convert them to peaceful uses.
* To permit the IAEA to verify the processes of dismantling and destruction of the nuclear explosive devices, as well as the destruction or conversion of the facilities for their production.
* Not to take any action to assist or encourage the dumping of radioactive wastes and other radioactive matter anywhere within the African nuclear-weapon-free zone
* To conclude a comprehensive safeguards agreement with the IAEA for the purpose of verifying compliance.
* To maintain the highest standards of security and effective physical protection of nuclear materials, facilities, and equipment to prevent theft or unauthorized use and handling. To that end each party undertakes to apply measures of physical protection equivalent to those provided for in the Convention on Physical Protection of Nuclear Material.

Protocol I requires the nuclear weapons States not to use or threaten to use a nuclear explosive device against any Party to the Treaty or any territory within the African nuclear-weapon-free zone for which a Party to Protocol III has international responsibility. Protocol II requires the nuclear weapons States not to test any nuclear explosive device anywhere in the African nuclear-weapon-free zone. Protocol III requires States with international responsibility for territories within the African nuclear-weapon-free zone (but not in the zone themselves) to respect all provisions of the Treaty insofar as those territories are concerned.

The Treaty permits each party to exercise its sovereign rights and to remain free to decide for itself whether to allow visits by foreign ships and aircraft to its ports and airfields, transit of its airspace by foreign aircraft, and navigation by foreign ships in its territorial sea or archipelagic waters in a manner not covered by the rights of innocent passage, archipelagic sea lane passage, or transit passage of straits.

The African Nuclear-Weapon-Free zone includes the entire continent of mainland Africa, and the following islands:

Agalega Island	Bassas da India

Canary Islands	Cape Verde
Cardagos Carajos Shoals	Chagos Archipelago - Diego Garcia
Comoros	Europa
Juan de Nova	Madagascar
Mauritius	Mayotte
Prince Edward & Marion Islands	Principe
Reunion	Rodrigues Island
Sao Tome	Seychelles
Tromelin Island	

Treaty of Bangkok – formally titled the ***"Treaty on the Southeast Asian Nuclear Weapon-Free Zone"*** the Treaty of Bangkok was [195]:

* Signed 15 December 1995.
* Treaty entered into force 27 March 1997

The following countries have signed and ratified the Treaty of Bangkok:

Brunei	Cambodia
Indonesia	Laos
Malaysia	Myanmar (Burma)
Philippines	Singapore
Thailand	Vietnam

None of the Nuclear Weapons States have yet ratified the Protocol to the Treaty.

The principal provisions of the Treaty on the Southeast Asian Nuclear Weapon-Free Zone include:

Each State Party undertakes not to:

* Develop, manufacture or otherwise acquire, possess or have control over nuclear weapons anywhere inside or outside the Zone
* Station or transport nuclear weapons by any means
* Test or use nuclear weapons
* Allow in its territory any other State to develop, manufacture or otherwise acquire, possess or have control over nuclear weapons
* Allow in its territory any other State to station, test, or use nuclear weapons
* Dump at sea or discharge into the atmosphere anywhere within the Zone any radioactive material or wastes, or allow any other State to do so.
* Dispose radioactive material or wastes on land in the territory of or under the jurisdiction of other States
* Provide source or special fissionable material or equipment or material especially designed or prepared for the processing, use, or production of special fissionable material to any State except under IAEA safeguards.

Each State Party undertakes to:

* Use exclusively for peaceful purposes nuclear material and facilities that are within its territory and areas under its jurisdiction and control
* Support the continued effectiveness of the Non-Proliferation Treaty and the IAEA Safeguards system.

The Protocol to the Treaty requires Nuclear Weapon States to undertake not to use or threaten to use nuclear weapons against any State Party to the treaty and not to use or threaten to use nuclear weapons anywhere within the Southeast Asia Nuclear Weapon-Free Zone.

The Treaty permits each party to exercise its sovereign rights and to remain free to decide for itself whether to allow visits by foreign ships and aircraft to its ports and airfields, transit of its airspace by foreign aircraft, and navigation by foreign ships in its territorial sea or archipelagic waters in a manner not covered by the rights of innocent passage, archipelagic sea lane passage, or transit passage of straits. Nothing in the Treaty shall prejudice the right of the States Parties to use nuclear energy.

The Southeast Asia Nuclear Weapon-Free Zone consists of the area comprising the territories of all States in Southeast Asia, namely, Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam, and their respective continental shelves and Exclusive Economic Zones.

In the "Almaty Declaration" of 28 February 1997, the leaders of five states in Central Asia (Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan) expressed their joint support for the formation of a nuclear weapon-free zone.[196] A treaty creating such a zone would be virtually identical to those creating the other four nuclear weapon-free zones. To date, a ***"Treaty on the Central Asian Nuclear Weapon-Free Zone"*** has not gone beyond initial draft stage.

Given the existence of the Treaty of Tlatelolco, the Treaty of Rarotonga, the Treaty of Bangkok, and the Antarctic Treaty, plus the probable entry into force of the Treaty of Pelindaba, almost all of the lands of the Southern Hemisphere are members of one nuclear weapon-free zone or another. Because of this there has been some talk of making the entire Southern Hemisphere into a single nuclear weapon-free zone.[196]

A number of other agreements have been signed which limit where and how nuclear weapons and other weapons of mass destruction may be used. These additional agreements include the Antarctic Treaty, the Outer Space Treaty, the Seabed Treaty, and the several Nuclear-Free Zone treaties. In this section we will take an abbreviated look at each of these treaties.

Antarctic Treaty – Formally titled the ***"The Antarctic Treaty"***, was [197]:

* Signed on 1 December 1959 by the United States, United Kingdom, Soviet Union, and many other states
* Ratified by the U. S. President on 18 August 1960
* Treaty entered into force on 23 June 1961

Countries of special note that have ratified or acceded to the Antarctic Treaty include:

Argentina	Australia	Austria
Belarus*	Belgium	Brazil
Bulgaria	Chile	China
Cuba	Czechoslovakia	Denmark
Ecuador	Finland	France
Germany	Greece	Hungary
India	Italy	Japan

Kazakhstan*	Republic of Korea	North Korea
Netherlands	New Zealand	Norway
Papua New Guinea	Peru	Poland
Romania	Russian Federation*	South Africa
Spain	Sweden	Ukraine*
United Kingdom	United States	* As USSR successor state

All countries with research stations and/or claims to territorial sovereignty have ratified the treaty. Countries of special note which have not signed or acceded to the Antarctic Treaty include:

Algeria	Egypt	Iran
Iraq	Pakistan	Sudan
Syria	Taiwan	

The principal provisions of the Antarctic Treaty include:

* Antarctica shall be used for peaceful purposes only. Establishment of military bases and fortifications, carrying out of military maneuvers, and testing of any kind of weapons is prohibited.
* Military personnel or equipment may be used for scientific research or other peaceful purposes.
* Any nuclear explosions in Antarctica and the disposal there of radioactive waste material shall be prohibited.
* All areas of Antarctica including all stations, installations, and equipment within these areas, and all ships and aircraft at points of discharging or embarking cargoes or personnel in Antarctica shall be open to inspection at all times.

This treaty does not affect any claims to territorial sovereignty in Antarctica. No new claims shall be made while this treaty is in force.

Outer Space Treaty – Formally titled the ***"Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies"***, the Outer Space Treaty was [51]:

* Signed on 5 August 1963 by the United States, United Kingdom, Soviet Union, and many other states
* Ratified by the U. S. President on 10 October 1963
* Treaty entered into force on 10 October 1963

Countries of special note that have ratified or acceded to the Outer Space Treaty include:

Argentina	Australia	Belarus
Brazil	Canada	Chile
China	Egypt	France
Germany	India	Iraq
Israel	Italy	Japan
Republic of Korea	Libya	Norway
Pakistan	Russian Federation	Singapore
South Africa	Spain	Sweden
Taiwan	Ukraine	United Kingdom
United States		

The list of ratifiers includes most but not all countries developing a space launch capability.

Countries of special note which have not ratified or acceded to the Outer Space Treaty include:

Algeria	Guyana	Indonesia
Iran	Kazakhstan	Malaysia
North Korea	Sudan	Zaire

The principal provisions of the Outer Space Treaty include:

* Exploration and use of outer space, including the moon and other celestial bodies shall be carried out for the benefit and in the interests of all countries.
* Outer space, including the moon and other celestial bodies shall be free for exploration and use by all states without discrimination.
* Outer space, including the moon and other celestial bodies is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.
* Parties will not place in orbit around the earth any objects carrying nuclear weapons or other weapons of mass destruction, install such weapons on celestial bodies or station such weapons in outer space in any other manner.
* The moon and other celestial bodies shall be used by all parties exclusively for peaceful purposes. Establishment of military bases, installations, and fortifications, the testing of any type of weapons, and the conduct of military maneuvers on celestial bodies shall be forbidden.
* Parties shall regard astronauts as envoys of mankind and render them all possible assistance in the event of accident, distress, or emergency landing on the territory of another, and provide for their prompt return to the state of registry of their spacecraft.
* Astronauts of one state shall render all possible assistance to astronauts of other states in carrying on activities in outer space.
* Non-governmental entities carrying out activities in space must be regulated by their responsible states. International organizations must be responsible for their activities as are all parties participating in such organizations.
* Parties who launch objects into space retain ownership of those objects under all conditions.
* Parties who launch objects into space are responsible for any damages caused to others by such objects.
* All stations, installations, equipment and space vehicles on the moon and other celestial bodies shall be open to representative of other states on a basis of reciprocity. Representatives shall give reasonable advance notice of visits.

Seabed Treaty – Formally titled the ***"Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Seabed and the Ocean Floor and in the Subsoil Thereof"***, the Seabed Treaty was [198]:

* Signed on 11 February 1971 by the United States, United Kingdom, Soviet Union, and many other states
* Ratification was advised by the U. S. Senate on 15 February 1972
* Ratified by the U. S. President on 26 April 1972
* Ratification document was deposited on 18 May 1972
* Treaty entered into force on 18 May 1972

Countries of special note that have ratified or acceded to the Seabed Treaty include:

Algeria	Australia	Belarus
Brazil	Canada	China
Cuba	Germany	India
Iran	Iraq	Japan
Republic of Korea	Russian Federation	South Africa
Taiwan	Turkey	Ukraine
United Kingdom	United States	

Countries of special note that have not signed or acceded to the Seabed Treaty include:

Argentina	Chile	Egypt
France	Libya	North Korea
Pakistan	Sudan	Syria

The principal provisions of the Seabed Treaty include:

Parties to this treaty shall:

* Not implant or emplace on the seabed or ocean floor or the subsoil thereof beyond the 12-mile limit, any weapon of mass destruction, or structures, launching installations, or others facilities designed for storing, testing, or using WMD.
* Not assist, encourage, or induce another state to implant or emplace weapons of mass destruction or associated structures on the seabed, ocean floor, or subsoil thereof.
* Have the right to verify through observations the activities of other states on the seabed or ocean floor provided such observation does not interfere with those activities.

This treaty shall not apply to activities conducted within the territorial waters of any state.

Missile Technology Control Regime

The **Missile Technology Control Regime** (MTCR) was established in 1987 by the United States and the other members of the G-7 economic group (United States, Canada, Germany, France, Italy, Japan, and United Kingdom).[199] The MTCR is not a treaty nor an international agreement. Rather it is a set of guidelines, mutually established and voluntarily followed by "member countries" for the restriction of proliferation (by controlling exports to proliferating countries) of missile technology capable of delivering weapons of mass destruction. Currently the following 29 countries are "members" of the MTCR:

Argentina	Australia	Austria
Belgium	Brazil	Canada
Denmark	Finland	France
Germany	Greece	Hungary
Iceland	Ireland	Italy
Japan	Luxembourg	Netherlands
New Zealand	Norway	Portugal
Russian Federation	South Africa	Spain
Sweden	Switzerland	Turkey
United Kingdom	United States	

Notably absent from this list are Belarus, China, Egypt, India, Iran, Iraq, Israel, North Korea, Pakistan, South Korea, and the Ukraine, all of which have significant missile programs and many of whom are known for their tendencies to proliferation. One unstated purpose of MTCR is to keep critical missile technology away from these countries.

The MTCR is implemented through its Guidelines.[200] The Guidelines define the purpose of the MTCR and provide identification of critical technology items and rules to guide member countries in making export decisions. "The purpose of the Guidelines is to limit the risks of proliferation of weapons of mass destruction (i.e., nuclear, chemical, and biological weapons), by controlling transfers that could make a contribution to delivery systems (other than manned aircraft) for such weapons." It is intended that all transfers of identified technology be treated on a case-by-case basis with due restraint and consideration of the likelihood that transferred technology would be put to use in peaceful versus WMD applications. The Regime is not intended to stifle or impede national space programs to the extent that those programs make no contributions to delivery systems for weapons of mass destruction. Since a satellite launch vehicle could be adapted for use as a WMD delivery system, it is clear that sound judgement must be exercised in the decision whether to permit a transfer. For example, a country with no history of WMD activity, no significant military weapons industry, and a substantial investment in satellite systems and space launch might be given favorable treatment with respect to a proposed transfer of missile technology; whereas a country with suspected clandestine WMD programs, no space launch industry, and a history of selling arms to other countries would not receive favorable treatment with respect to the same proposed transfer.

The Equipment and Technology Annex to the Guidelines identifies twenty items of technology critical to missile and unmanned air vehicle systems. These items are divided into two categories. Category I items are complete missile or air vehicle systems or complete major subsystems that could be immediately incorporated into potential delivery systems for WMD. It is expected that most proposals for transfer of Category I items would be denied. Category II items are generally critical components required for complete delivery systems. There is more potential for peaceful use of these components and more likelihood of approval for their transfer. A rough description of the items contained in each Category is provided below. The Annex should be consulted for more detail.

Category I

1. Complete rocket systems and unmanned air vehicle systems capable of delivering a 500 kg payload to a range of at least 300 km as well as specially designed production facilities for these.

2. Complete subsystems usable in Item 1 as well as specially designed production facilities for these, to include:

- individual rocket stages
- reentry vehicles and component specially designed for reentry vehicles
- rocket engines having total impulse greater than 1.1 MN-s
- guidance sets capable of CEP < 3.33 % of range
- thrust vector control subsystems
- safing, arming, fuzing, and firing mechanisms

Category II

3. Propulsion components or specially designed production facilities.

4. Propellants and constituents.

5. Production technology or production equipment for production, handling, processing, or acceptance testing of liquid propellants or solid propellants.

6. Equipment, technical data, and procedures for the production of structural composites usable in missile systems.

7. Pyrolytic deposition and densification equipment.

8. Structural materials usable in missile systems.

9. Instrumentation, navigation, and direction finding equipment.

10. Flight control systems.

11. Avionics equipment, technology, and components.

12. Launch support equipment.

13. Analog or digital computer systems which are either rated for use at temperatures > -45 C and < +55 C or are designed to be radiation hardened.

14. Analog-to-digital converters with >= 8 bit resolution which are either MILSPEC or radiation hardened or rated for operation at temperatures from -45 to +55 C.

15. Test facilities.

16. Specially designed software/computers for modeling, simulation, or design integration of missile systems.

17. Materials for reducing observables such as radar reflectivity, ultraviolet/infrared signatures, and acoustic signatures.

18. Devices for protecting missile systems against nuclear effects.

19. Complete rocket or unmanned air vehicle systems not covered in Item 1 and capable of a maximum range > 300 km.

20. Complete subsystems usable in Item 19 but not in systems in Item 1.

ABM Treaty

The **ABM Treaty** limited a potential arms race over the development and deployment of anti-ballistic missile (ABM) systems whose purpose was to destroy enemy ICBMs and/or reentry vehicles. Formally titled the ***"Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems"***, the ABM Treaty was [21]:

* Signed on 26 May 1972 by the United States and the Soviet Union
* Ratified by the U. S. President on 30 September 1972
* Treaty entered into force on 3 October 1972

NOTE ADDED PRIOR TO PRINTING: As of December 2001, the Bush administration informed the Russian government that the U. S. was withdrawing from the ABM Treaty. However, the U. S. Congress has indicated that it will consider the matter and may pass legislation that restores the treaty obligations.

The principle provisions of the ABM Treaty include:

Each party undertakes not to:

* Deploy ABM systems for a defense of the territory of its country nor provide a base for such a defense, not deploy ABM systems for defense of an individual region except as provided for in this treaty.
* Develop, test, or deploy ABM systems or components which are sea-based, air-based, space-based, or mobile land-based.
* Deploy ballistic missile early warning radars except along the periphery of its national territory and oriented outward.
* Develop, test, or deploy launchers with multiple launch or rapid reload.
* Give missiles, launchers, or radars, other than ABM components, capabilities to counter strategic ballistic missiles in flight.

Each party is permitted:

* One ABM system deployment area with 150 km radius centered on the national capital and having no more than 100 ABM launchers and 100 ABM interceptors at the launch sites, and ABM radars within no more than 6 3 km diameter circular complexes.
* One ABM system deployment area with 150 km radius and having no more than 100 ABM silo launchers and 100 ABM interceptor missiles at the launch sites, two large phased-array ABM radars comparable in potential to ABM radars operational or under construction on the date of signature of this treaty, and 18 ABM radars having a potential less than the smaller of the two large ABM radars.
* Up to 15 launchers at ABM test ranges.

The "***Agreed Statements, Common Understandings, and Unilateral Statements Regarding the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems***" was signed by both parties on 26 May 1972.[201] The primary technical result of this document is that both parties agreed not to deploy phased array radars with mean emitted power times antenna area that exceeds 3 million watt-square meters unless those radars are used exclusively to track objects in deep space or as part of national technical means of verification. This is equivalent to a radar with an 10 m by 10 m antenna emitting an average power of 30 kW. This is large but not excessively so.

The "***Protocol to the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems***" was:[202]

* Signed on 3 July 1974 by the United States and the Soviet Union.
* Ratified by the U. S. President on 19 March 1976.
* Protocol entered into force on 24 May 1976.

The principle provision of this protocol was to limit each party to one of the two ABM deployment areas permitted in the original treaty. The U.S.S.R. selected Moscow as its deployment site and the U.S. selected Grand Forks, ND (near to bases containing a number of ICBM missile launching silos).

The "***Memorandum of Understanding Relating to the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems of May 26, 1972***" was released on 26 September 1997.[203] By this memorandum the United States, Ukraine, Belarus, Kazakhstan, and the Russian Federation agreed to become parties to the ABM Treaty. The Lisbon Protocol to the Strategic Arms Reduction Treaty (START)entered into force on 5 December 1994. It identified Ukraine, Belarus, Kazakhstan, and the Russian Federation as successor states to the former Soviet Union, and bound them to comply with START and with the Nuclear Non-Proliferation Treaty. The Lisbon Protocol has been used as justification for extending all agreements between the U. S. and U.S.S.R. to include the new states as successor states.

The "***Standing Consultative Commission Second Agreed Statement Relating to the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems of May 26, 1972***" was released on 26 September 1997.[204] The parties agreed:

* During tests of higher-velocity ($V_{INT} > 3$ km/s) theater missile defense (TMD) systems:
  - the velocity of the target missiles will not exceed 5.0 km/s
  - the range of the target missiles will not exceed 3500 km.
* Not to develop, test, or deploy space-based theater missile defense interceptor missiles or space-based theater missile defense based on "other physical principles" (such as lasers).

The implication of the Second Agreed Statement is that if a theater missile defense system has an inherent ABM capability (either by accident or design), then that capability can never be tested against an ICBM. Lack of successful ICBM testing would sustain doubts as to the true capability and probably prevent deployment of the system in an ABM role.

The ABM treaty is reviewed regularly. As a result of these reviews there are many other memoranda, agreed statements, unilateral statements, etc. that bear on the law. Those which address true proliferation issues have been discussed above. The others may be found on the Internet at the Worldwide Web site for the treaty.[21]

Strategic Arms Limitation Treaties (SALT) and Reduction Treaties (START)

The nuclear-related treaties and conventions described in the earlier sections of this chapter have almost exclusively dealt with the reduction or prevention of the spread of nuclear weapons to countries, regions, or applications where they were not already entrenched. In the 1970's, 1980's, and 1990's the United States and the Soviet Union conducted a number of bilateral negotiations aimed at limiting the nuclear arms race between the two superpowers. The arms limitation and reduction treaties discussed in this section placed limits on already proliferated strategic nuclear forces and ultimately forced significant reductions in quantities of deployed and stockpiled nuclear weapons.

The first of these negotiations was the Strategic Arms Limitation Talks (SALT).[205] Considerable progress was achieved, but many stumbling blocks remained. The primary outputs of the first SALT negotiations were the ABM treaty, the interim "**SALT I**" Treaty, and agreement to continue with further SALT negotiations. Formally titled the **"*Interim Agreement Between the United States of America and the Union of Soviet Socialist Republics on Certain Measures With Respect to the Limitation of Strategic Offensive Arms*"**, the SALT I Treaty was:[206]

* Signed on 26 May 1972 by the United States and the Soviet Union
* Approved by the U. S. President on 30 September 1972
* Agreement entered into force on 3 October 1972.

The principle provisions of the SALT I Treaty included:

* Neither side will begin construction of additional fixed land-based ICBM launchers
* Neither side will convert light ICBM launchers into heavy ICBM launchers
* The U. S. is limited to a total of 1054 land-based ICBMs
* The U. S. S. R. is limited to a total of 1618 land-based ICBMs
* The U. S. may deploy no more than 710 SLBM launchers on 44 submarines
* The U. S. S. R. may deploy no more than 950 SLBM launchers on 62 submarines

No limitations on mobile ICBMs were established.

The second set of SALT talks led to an agreement to limit nuclear forces to levels even lower than the SALT I levels and to agreement to enter into nuclear arms reduction negotiations. Formally titled the **"*Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Strategic Offensive Arms*"**, the **SALT II** Treaty was:[207]

* Signed on 18 June 1979 by the United States and the Soviet Union
* Treaty was never ratified.

The principle provisions of the SALT II Treaty included:

* An aggregate limit on the number of strategic nuclear delivery vehicles (ICBM launchers, SLBM launchers, heavy bombers, and long-range (>600 km range) air-to-surface ballistic missiles (ASBMs)) of 2250 for each side.
* An aggregate limit of 1320 launchers with MIRVed ballistic missiles and heavy bombers with long-range cruise missiles for each side
* An aggregate limit of 1200 launchers of MIRVed ICBMs and MIRVed SLBMs for

each side
* An aggregate limit of 820 launchers of MIRVed ICBMs for each side
* No construction of additional fixed ICBM launchers
* No heavy mobile ICBM launchers, no heavy SLBM launchers, and no heavy ASBM launchers
* No flight-testing or deployment of new types of ICBM, with the exception of one new type of light ICBM for each side
* No increasing the number of warheads on existing ICBMs, a limit of 10 warheads on the new ICBM permitted each Party, a limit of 14 warheads on SLBMs, and 10 warheads on ASBMs
* An average limit of 28 cruise missiles per bomber with no more than 20 cruise missiles on each existing bomber
* Limitations on the launch weight and throw weight of ballistic missiles
* A ban on the Soviet SS-16 ICBM
* A ban on rapid reload ICBM launch systems

Shortly after the SALT II Treaty was sent to the U. S. Senate for ratification, the President requested that ratification be delayed due to the Soviet invasion of Afghanistan. Subsequent findings that the Soviet Union had not lived up to its commitment to abide by the treaty provisions, precluding ratification. However, the U. S. agreed to continue to abide by the SALT II limits unless Soviet violations of the Treaty provisions were deemed to warrant their abandonment.

After many years of continued negotiations, now called the Strategic Arms Reduction Talks (**START**), an agreement was reached which promised actual reductions in strategic nuclear weapons, not just limits. This followed the successful total elimination of intermediate range nuclear weapons, as discussed below. Formally titled the **"*Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms*"**, the START Treaty was:[208]
* Signed on 31 July 1991 by the United States and the Soviet Union
* Lisbon Protocol signed on 23 May 1992 by United States and the successor states to the Soviet Union
* Treaty entered into force on 5 December 1994.

The principal provisions of the START Treaty include:
Each Party:
* Shall reduce and limit its ICBMs and ICBM launchers, SLBMs and SLBM launchers, heavy bombers, ICBM warheads, SLBM warheads, and heavy bomber armaments so that the aggregate numbers do not exceed:
    - 1600, for deployed ICBMs and associated launchers, deployed SLBMs and associated launchers, and deployed heavy bombers, including 154 for heavy ICBMs and their associated launchers.
    - 6000, for warheads attributed to deployed ICBMs, deployed SLBMs, and deployed heavy bombers, including:
        — 4900 for warheads attributed to deployed ICBMs and deployed SLBMs
        — 1100 for warheads attributed to deployed ICBMs on mobile launchers

— 1540 for warheads attributed to deployed heavy ICBMs.

* Shall limit the aggregate throw-weight of its deployed ICBMs and deployed SLBMs to be less than 3600 metric tons.
* Shall limit the aggregate number of non-deployed ICBMs for mobile launchers to no more than 250; within this limit the number of non-deployed ICBMs for rail-mobile launchers shall not exceed 125.
* Shall limit the aggregate number of non-deployed mobile launchers of ICBMs to no more than 110; within this limit the number of non-deployed rail-mobile launchers of ICBMs shall not exceed 18.
* Shall limit the number of ICBMs and SLBMs located at test ranges to no more than 25.
* Shall limit the number of test launchers to no more than 25 fixed launchers and 20 mobile launchers.
* Shall limit the number of non-deployed mobile launchers at training sites to no more than 40; training launchers must contain only training models of missiles.
* Shall limit the number of silo training launchers and mobile training launchers to no more than 60; training launchers must contain only training models of missiles.
* Shall limit the number of heavy bombers equipped for non-nuclear armaments and training heavy bombers to no more than 75.

Each Party undertakes not to:

* Produce, flight-test, or deploy heavy ICBMs of a new type.
* Produce, flight-test, or deploy heavy SLBMs
* Produce, test, or deploy mobile launchers of heavy ICBMs
* Produce, flight-test, or deploy an ICBM or SLBM with more than 10 reentry vehicles.
* Flight-test from space launch facilities ICBMs or SLBMs equipped with reentry vehicles.
* Produce, test, or deploy systems for rapid reload of launchers.
* Produce, test, or deploy air-to-surface ballistic missiles.
* Produce, test, or deploy long-range nuclear ALCMs with two or more warheads.
* Flight test with nuclear armaments any aircraft that is not an airplane that has a range of 8000 km or more.
* Have underground facilities accessible to ballistic missile submarines.

For purposes of counting towards the maximum aggregate limits:

* Each deployed ICBM and its associated launcher shall be counted as one unit.
* Each deployed SLBM and its associated launcher shall be counted as one unit.
* Each deployed heavy bomber shall be counted as one unit.
* Each deployed launcher of ICBMs shall be considered to contain one deployed ICBM.
* Each deployed launcher of SLBMs shall be considered to contain one deployed SLBM.
* Ballistic missiles separated from their launchers shall be considered to be contained in those launchers.
* The number of warheads attributed to an ICBM or SLBM of each existing type shall be the number specified in the *Memorandum of Understanding*.
* The number of warheads attributed to a new ICBM or SLBM shall be the maximum number of reentry vehicles with which that missile has been flight tested.
* Each reentry vehicle is considered to be one warhead.

* Each U. S. heavy bomber equipped with long-range nuclear ALCMs up to a total of 150 shall be attributed to have 10 warheads.
* Each U. S. heavy bomber equipped with long-range nuclear ALCMs in excess of 150 shall be attributed to have a number of warheads equal to the number of long-range nuclear ALCMs for which it is actually equipped.
* Each Russian heavy bomber equipped with long-range nuclear ALCMs up to a total of 180 shall be attributed to have 8 warheads.
* Each Russian heavy bomber equipped with long-range nuclear ALCMs in excess of 180 shall be attributed to have a number of warheads equal to the number of long-range nuclear ALCMs for which it is actually equipped.
* Each heavy bomber equipped for nuclear armaments other than long-range nuclear ALCMs shall be attributed with one warhead.

The START Treaty also places severe restrictions on the basing of mobile ICBMs. To facilitate treaty verification, flight tests of ICBMs or SLBMs shall not deny access to telemetry by any means, including encryption, jamming, narrow directional beaming, or encapsulation of telemetric data in ejectable capsules or reentry vehicles. There are a number of provisions requiring advance notification of changes in deployment or tests. Additional provisions give each Party the right to conduct a number of on-site inspections of missiles, launchers, warheads, test facilities, and disposal facilities.

The ***"Protocol on Procedures Governing the Conversion or Elimination of the Items Subject to the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms"*** [209] spells out explicit mechanisms for accomplishing the reduction of offensive arms.

Warheads shall be removed from ICBMs before destruction. The following may be removed before destruction:
* electronic and electromechanical devices of the guidance and control system.
* propellant from the stages.
* auxiliary pyrotechnic devices.
* penetration aids.
* propulsion units from the warhead dispensing mechanism.

If solid fuel has not been removed from stages, the stages shall be destroyed by explosive demolition or burning. Rocket motor nozzles and cases and interstage skirts shall be crushed, flattened, cut into two pieces of roughly equal size, or destroyed by explosion. The warhead dispensing mechanism shall be crushed, flattened, cut into pieces of two roughly equal sizes, or destroyed by explosion. Launch canisters shall be crushed, flattened, cut into multiple pieces, or destroyed by explosion.

Silo launchers shall be destroyed by removing, dismantling, or destroying the silo door and destroying the silo headworks. The headworks may be destroyed by excavation to a depth of at least 8 meters or by explosion to a depth of at least 6 meters. The silo may be filled to the level of the bottom of the excavation or explosion crater.

Road-mobile launchers shall be destroyed by:

* Removing the erector-launcher mechanism and leveling supports from the launcher chassis
* The framework of the erector-launcher on which the ICBM is mounted shall be cut at locations that are not assembly joints into two pieces of approximately equal size.
* Launch support equipment, including external instrumentation compartments, shall be removed.
* The mountings of the erector-launcher and of the launcher leveling supports shall be cut off the launcher chassis and each such mounting shall be cut at a location that is not an assembly joint into two pieces of approximately equal size.
* A portion of the self-propelled chassis at least 0.78 meters in length shall be cut off aft of the rear axle, and that portion shall be cut into two pieces of approximately equal size.

Rail-mobile launchers shall be destroyed by:

* Removing the erector-launcher mechanism from the railcar
* The framework of the erector-launcher on which the ICBM is mounted shall be cut at locations that are not assembly joints into two pieces of approximately equal size.
* Launch support equipment, including external instrumentation compartments, shall be removed.
* The railcar shall be cut at locations that are not assembly joints into two pieces of approximately equal size.

SLBM launchers shall be eliminated by removing the missile section from the submarine or by following these steps:

* The missile launch tubes, and all elements of their reinforcement, including hull liners and segments of circular structural members between the launch tubes, as well as the entire portion of the pressure hull, the entire portion of the outer hull, and the entire portion of the superstructure through which all the missile launch tubes pass and that contain all the missile launch tube penetrations shall be removed from the submarine.
* Missile launch tubes that have been removed shall be cut into pieces of approximately equal size.

Upon completion of these steps, the submarine may be used for other purposes after:

* Installing a section without SLBM missile launch tubes and penetrations for them, and without SLBM missile launch-tube reinforcements.
* Replacing the entire portion of the pressure hull, the entire portion of the outer hull, and the entire portion of the superstructure that were removed with portions without SLBM missile launch tubes and penetrations for them, and without SLBM missile launch-tube reinforcements.

Such submarines shall differ from ballistic missile submarines on the basis of external differences observable by national technical means.

The elimination of heavy bombers shall be accomplished in the following manner:

* The tail section with tail surfaces shall be severed from the fuselage at a location obviously not an assembly joint.
* The wings shall be separated from the fuselage at any location by any method.
* The remainder of the fuselage shall be severed into two pieces within the area of attachment of the wings to the fuselage at a location obviously not an assembly joint.

Formally titled the "***Protocol to the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms***", the **Lisbon Protocol** was:[180]

* Signed on 23 May 1992 by the United States, Belarus, Kazakhstan, Russian Federation, and the Ukraine

The protocol held that the successor states to the former Soviet Union would abide by all provisions of the recently signed treaties, specifically the START Treaty and the Nuclear Proliferation Treaty. The Lisbon Protocol has been tacitly assumed to bind the successor states to all Treaties concluded with the former Soviet Union. This assumption does not have any legal standing, but does have considerable political significance. Violations of any Soviet Union treaty by any of the successor states would bring serious repercussions to that state from the world community.

Formally titled the "***Treaty Between the United States of America and the Union of Soviet Socialist Republics on Further Reduction and Limitation of Strategic Offensive Arms***", the **START II** Treaty was:[210]

* Signed on 3 January 1993 by the United States and the Soviet Union
* Ratification advised by the U. S. Senate on 26 January 1996
* Treaty entered into force on ? (Ratified by the Russian Duma on 14 April 2000)

The principal provisions of the START II Treaty include:

Each Party:

* Shall reduce and limit its ICBMs and ICBM launchers, SLBMs and SLBM launchers, heavy bombers, ICBM warheads, SLBM warheads, and heavy bomber armaments, so that aggregate numbers for each Party shall not exceed:
    - 3500 total strategic warheads.
    - 1750 warheads attributed to deployed SLBMs.
    - 0 warheads attributed to deployed ICBMs of types to which more than one warhead is attributed (i.e., no MIRVed ICBMs).
    - 0 warheads attributed to heavy ICBMs.
* Shall eliminate all of its heavy ICBMs and their launch canisters. SS-18s must be eliminated.
* Subject to aggregate limits, may convert MIRVed ICBMs (except heavy ICBMs) to single warhead ICBMs. For example, Minuteman III and SS-19 missiles may be converted.
* Subject to downloading limits, may load MIRVed SLBMs with fewer warheads each to satisfy total limits. Basically, Trident and SS-N-18 missiles may be redeployed with fewer warheads.
* Not to produce, acquire, flight-test (except for flight tests from space launch facilities for the purpose of lifting items into space), or deploy ICBMs to which more than one warhead is attributed. Under this provision, Peacekeeper and SS-24 ICBMs must be destroyed or used only as space launch vehicles.

Except for the items listed above, the provisions of the START Treaty remain basically unchanged by START II.

Upon the entry into force of the START II Treaty, both the United States and the Russian Federation are committed to begin negotiations on a third round of arms reductions talks, nominally called START III. As of Summer 2000, these negotiations had not yet begun. A reduction in the total number of allowable warheads to values in the range of 1500-2500 is a distinct possibility. The START III Treaty will undoubtedly require START IV negotiations to begin as soon as it becomes effective.

While negotiations on limiting strategic arms were being conducted, the planned deployment of ground-launched cruise missiles (GLCMs) and Pershing II ballistic missiles into Western Europe coupled with the Soviet deployment of SS-20 ballistic missiles threatened serious instability. This created a unique opportunity for the first, zero-zero arms control agreement. Zero-zero agreements mean that both sides completely eliminate certain weapons from their inventories.

Formally titled the **"*Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Elimination of Their Intermediate-Range and Shorter-Range Missiles*"**, the **Intermediate Nuclear Forces (INF) Treaty** was:[154]

* Signed on 8 December 1987 by the United States and the Soviet Union
* Ratification advised by the U. S. Senate on 27 May 1988
* Instruments of ratification exchanged on 1 June 1988
* Entered into force on 1 June 1988
* Proclaimed by U. S. President on 27 December 1988

The first principle provision of this treaty was the complete elimination of all shorter range (500 to 1000 km range) and intermediate range (1000 to 5500 km range) ground-launched ballistic and cruise missiles. This meant elimination (destruction not just removal from active deployment) of the U. S. Pershing IA and Pershing II ballistic missiles and BGM-109G (GLCM) cruise missiles and the Soviet SS-20, SS-4, SS-5, SS-12, and SS-23 ballistic missiles. The second principle provision is the prohibition on developing any future ground-launched missiles with ranges between 500 and 5500 km range. The elimination was overseen by on-site inspections and involved total physical destruction of all major missile components and launcher systems using techniques similar to those specified in the later START treaties.

The **"*Fissile Material Production Cut-off Treaty*"** [211] is a proposal currently under consideration by the Geneva-based Conference on Disarmament. The basic tenet of such a treaty would be to ban further production of highly enriched uranium and plutonium for use in nuclear weapons. It would place quantitative limits on the quantity of highly enriched material a State could have and it would place all fissile material enrichment and production facilities under IAEA Safeguards. A draft of such a treaty has not yet been circulated for comment and negotiation.

Environmental Modification Convention

The **Environmental Modification Convention** (or EMC) is the primary international agreement for preventing environmental modification as a means of warfare. Formally titled the ***"Convention on the Prohibition of Military or any Other Hostile Use of Environmental Modification Techniques"***, the EMC was [117]:

* Signed on 18 May 1977 by the United States, United Kingdom, Soviet Union, and many other states
* Ratified by the U. S. President on 13 December 1979
* Treaty entered into force on 5 October 19*78*

Countries which have ratified or acceded to the EMC include:

Afghanistan	Algeria	Antigua & Barbuda
Argentina	Australia	Austria
Bangladesh	Belarus	Belgium
Benin	Brazil	Brunei
Bulgaria	Canada	Cape Verde
Chile	Cuba	Cyprus
Czech Republic	Denmark	Dominica
Egypt	Finland	Germany
Ghana	Greece	Guatemala
Hungary	India	Ireland
Italy	Japan	Republic of Korea
Kuwait	Laos	Malawi
Mauritius	Mongolia	Netherlands
New Zealand	Niger	North Korea
Norway	Pakistan	Papua New Guinea
Poland	Romania	Russian Federation(as USSR)
St. Christopher-Nevis	Saint Lucia	St. Vincent & Grenadines
Sao Tome & Principe	Solomon Islands	Spain
Sri Lanka	Sweden	Switzerland
Tunisia	Ukraine	United Kingdom
United States	Uruguay	Vietnam
Yemen		

Countries which have signed but not ratified the EMC include:

Bolivia	Ethiopia	Holy See
Iceland	Iran	Iraq
Lebanon	Liberia	Luxembourg
Morocco	Nicaragua	Portugal
Sierra Leone	Syria	Turkey
Uganda	Uzbekistan	Zaire

Countries of special note which have neither signed nor acceded to the EMC include:

Burma (Myanmar)	China	France
Indonesia	Israel	Libya
Mexico	Panama	Singapore
South Africa	Sudan	Taiwan
Thailand	Venezuela	

The principal provisions of the Environmental Modification Convention include:

Parties to this Convention undertake not to:

* Engage in any military or any other hostile use of environmental modification techniques having widespread, long-lasting, or severe effects as the means of destruction, damage, or injury to any other party.
* Assist, encourage, or induce any state, group of states, or international organization to engage in activities contrary to this Convention.

Parties to this convention undertake to:

* Facilitate, and have the right to participate in, the fullest possible exchange of scientific and technological information on the use of environmental modification techniques for peaceful purposes.
* Take any measures it considers necessary to prohibit or prevent any activity in violation of this Convention anywhere under its jurisdiction.

The provisions of this convention shall not hinder the use of environmental modification techniques for peaceful purposes.

Open Skies Treaty

The **Open Skies Treaty** would permit the overflight of the sovereign territory of any state by aircraft equipped with specific sensor technologies for the verification of arms control treaties. Failure of a similar measure in the late 1950's led to the development of spy satellites to overfly the sovereign territory of other states to acquire photographs of military developments. This action was of sufficiently questionable legality that official acknowledgment of the capability was not made for four decades. The Open Skies Treaty is intended to reduce many of the uncertainties and difficulties associated with satellite systems and to make verification technology available to nations without major space programs. The treaty addresses only the geographical regions of concern to NATO and the former Warsaw Pact countries.

Formally titled the ***"Treaty on Open Skies"***,[212] the Open Skies Treaty was:

* Signed on 24 March 1992 by the United States, Russian Federation, United Kingdom, and many others
* Ratified by the United States on 3 December 1993.
* Treaty has not yet entered into force due to the failure to achieve ratification by Belarus, Ukraine, and the Russian Federation (who are required for entry into effect).

Countries that have signed and ratified the Open Skies Treaty include:

Belgium	Bulgaria	Canada
Czech Republic	Denmark	France
Germany	Greece	Hungary
Iceland	Italy	Luxembourg
Netherlands	Norway	Poland
Portugal	Romania	Slovak Republic
Spain	Turkey	United Kingdom
United States		

Countries that have signed but not ratified the Open Skies Treaty include:

Belarus	Georgia	Kyrgyzstan
Russian Federation	Ukraine	

The treaty is open to signature by the following countries, which have not yet done so:

Armenia	Azerbaijan	Kazakhstan
Moldova	Tajikistan	Turkmenistan
Uzbekistan		

The principle provisions of the Open Skies Treaty include:

Each State Party agrees:

* To accept (if requested to do so) a number of observation flights over its territory by States Parties in accordance with the provisions of this treaty up to limits defined by the "passive quotas" in Annex A. The maximum passive quota for any State has been initially agreed to be 42 flights. Many states have much smaller passive quotas. In the initial distribution, the sum of the active quotas of all other States has seldom approached the passive quota for any State.
* To have the right (if it desires to do so) to conduct observation flights over the territories of other States Parties in accordance with the provisions of this treaty up to limits defined by the "active quotas" in Annex A.

* That the total active quota of any State Party shall not exceed its total passive quota.
* That a State Party has the right (if it desires to do so) to conduct a number of observation flights over the territory of another State Party as that other State Party has the right to conduct observation flights over the territory of the first State Party.
* The Open Skies Consultative Commission shall meet annually to review and renegotiate the quotas.
* Observation aircraft will be equipped only with sensor from among the following categories:
    - optical panoramic and framing cameras
    - video cameras with real-time display
    - infrared line-scanning devices
    - sideways-looking synthetic aperture radar (SAR).
* Optical and panoramic cameras shall not have a ground resolution better than 30 cm at the minimum height above ground. The aircraft shall have no more than one panoramic camera, one down-looking framing camera, and two obliquely-looking framing cameras (one on either side) providing coverage of the ground up to 50 km on each side of the aircraft.
* Video cameras will not have a ground resolution better than 30 cm at minimum height above ground.
* Infrared line-scanning devices shall not have a ground resolution better than 50 cm at the minimum height above ground. Only one such device is permitted.
* SAR sensors shall not have a ground resolution better than 3 m. Only one such device is permitted. It may look from either side of the aircraft but not both simultaneously.
* Sensors for the collection, processing, retransmission, or recording of electronic signal from electromagnetic waves are prohibited on the observation aircraft (except for such equipment as is required for operation of the allowed sensor types)
* Sensors must have covers that can only be removed external to the aircraft to prevent data acquisition prior to the specified observation flight.
* Sensors used must be commercially available to all States Parties to the Treaty.
* The observed country must be notified 72 hours in advance of the arrival of an observation team.
* Observation flights must begin and end at specified “Open Skies” airfields and cannot cannot cover greater ground distances than specified for each airfield.
* The observed country has the right to inspect the observation aircraft before and after the observation flight.
* The observed country has the right to place at least two flight monitors and one interpreter on board the observation aircraft. If the aircraft exceeds 35,000 kg gross takeoff weight, then an additional monitor is permitted for each on-board sensor control station.
* Observation flights take precedence over regularly scheduled flights.
* The observing party must file a detailed flight plan that observes the maximum flight distance and minimum height above ground requirements necessary for limiting sensor ground resolution.

Convention on Conventional Weapons (CCW)

In 1980 the Nations of the World convened in Geneva to address prohibiting certain conventional weapons that were deemed to have indiscriminate effects or to cause unnecessary suffering. The first output of this conference, concluded on 10 October 1980, was the **Convention on Conventional Weapons (CCW)**. Properly called the ***"Convention on Prohibition or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to have Indiscriminate Effects"***, the convention was opened for signature on 10 April 1981 and entered into force on 2 December 1983. [243] The original convention had three separate protocols: Protocol I on Non-Detectable Fragments, Protocol II on Mines, and Protocol III on Incendiary Weapons.[244] The United States signed the convention on 8 April 1982 and the U. S. Senate ratified Protocols I and II in March 1995. On 3 May 1996, the First Review Conference for the CCW completed its review and adopted amendments to Protocol II and accepted a new Protocol IV on Blinding Laser Weapons.[245] The United States ratified the amended Protocol II on 24 May 1999, but has failed to ratify either Protocol III or Protocol IV.

The following list summarizes the ratification and/or accession status of each Protocol. [246] After the name of each nation is a parenthetic list of numbers. The numeral 1 denotes ratification of Protocol I, 2 denotes ratification of Protocol II, 3 denotes ratification, of Protocol III, 4 denotes ratification of Protocol IV, and A denotes ratification of amended Protocol II. Thus (1234A) denotes acceptance of all five protocols.

Argentina (1234A)	Australia (1234A)	Austria (1234A)
Bangladesh (1234A)	Belarus (1234)	Belgium (1234A)
Benin (13)	Bosnia-Herzegovina (123A)	Brazil (1234A)
Bulgaria (1234A)	Cambodia (1234A)	Canada (1234A)
Cape Verde (1234A)	China (1234A)	Colombia (1234A)
Costa Rica (1234A)	Croatia (123)	Cuba (123)
Cyprus (123)	Czech Republic (1234A)	Denmark (1234A)
Djibouti (123)	Ecuador (123A)	El Salvador (1234A)
Estonia (134A)	Finland (1234A)	France (124A)
Macedonia (123)	Germany (1234A)	Georgia (123)
Greece (1234A)	Guatemala (123)	Holy See (1234A)
Hungary (1234A)	India (1234A)	Ireland (1234A)
Israel (12)	Italy (1234A)	Japan (1234A)
Jordan (13A)	Laos (123)	Latvia (1234)
Lesotho (123)	Liechtenstein (1234A)	Lithuania (134A)
Luxembourg (1234A)	Maldives (1234A)	Malta (123)
Mauritius (123)	Mexico (1234)	Moldova (1234A)
Monaco (1A)	Mongolia (1234)	Netherlands (1234A)
New Zealand (1234A)	Niger (123)	Norway (1234A)
Pakistan (123A)	Panama (1234A)	Peru (134A)
Philippines (1234A)	Poland (123)	Portugal (123A)
Romania (123)	Russian Federation (1234)	Senegal (3A)
Seychelles (1234A)	Slovakia (1234A)	Slovenia (123)
South Africa (1234A)	Spain (1234A)	Sweden (1234A)
Switzerland (1234A)	Tajikistan (1234A)	Togo (123)

Tunisia (123)	Uganda (123)	Ukraine (123A)
United Kingdom (1234A)	United States (12A)	Uruguay (1234A)
Uzbekistan (1234)	Yugoslavia (123)	

Protocol I (***Protocol on Non-Detectable Fragments***) to the Convention quite simply prohibits the use of any weapon the primary effect of which is to injure by fragments which in the human body escape detection by x-rays. That is, shrapnel from fragmentation weapons, bullets, or other projectiles cannot be made of plastics which are have opacity similar to human soft tissues and are thus undetectable by x-rays.

Protocol II (***Protocol on Prohibitions or Restrictions on the Use of Mines, Booby Traps and Other Devices***) addresses mines, booby-traps, and other similar devices. In general, it is prohibited to direct such weapons against the civilian population or against individual civilians. Indiscriminate use is also prohibited. Indiscriminate use is any placement of such weapons which is not on or directed at a military objective, which employs a means of delivery which cannot be directed at a specific military objective, or which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated. Specifically it is prohibited:

* To use mines in any city, town, village, or other are containing a similar concentration of civilians in which combat between ground forces is not taking place or does not appear imminent, unless they are placed on or in the close vicinity of a military objective or unless measures are taken to protect the civilians from their effects.
* To use remotely delivered mines unless such mines are only used within an area which is a military objective and unless their location can be accurately recorded or each mine has an effective neutralizing mechanism that will render them harmless or destroy themselves after the mine no longer serves the military purpose for which it was emplaced.
* To use any booby-trap in the form of an apparently harmless portable object which is specifically designed and constructed to contain explosive material and to detonate when it is disturbed or approached.
* To use booby-traps which are in any way attached to or associated with:
    - i. internationally recognized protective emblems, signs, or signals
    - ii. sick, wounded, or dead persons
    - iii. burial or cremations sites or graves
    - iv. medical facilities, medical equipment, supplies, or medical transportation
    - v. children's toys or other portable objects or products designed for the feeding, health, hygiene, clothing, or education of children
    - vi. food or drink
    - vii. kitchen utensils or appliances except in military establishments, locations, or supply depots
    - viii. objects clearly of a religious nature
    - ix. historic monuments, works of art, or places of worship that constitute the cultural or spiritual heritage of peoples
    - x. animals or their carcasses.
* To use booby-traps which are designed to cause superfluous injury or unnecessary

suffering.

Parties to a conflict shall record the location of all pre-planned minefields laid by them and all areas in which they have made large-scale and pre-planned use of booby-traps. Parties shall endeavor to ensure the recording of all other minefields, mines, and booby-traps which they have laid or placed in position. Such records shall be retained and made available to all affected parties. After the cessation of active hostilities, the parties shall endeavor to reach agreement on actions necessary to remove or otherwise render ineffective, all minefields, mines, and booby-traps placed in position during the conflict.

The amendments to Protocol II require the following additions. Each Party is responsible for all mines, booby-traps, or other devices employed by it and undertakes to clear, remove, destroy, or maintain them. Mines, booby-traps, or other devices designed to explode based on any non-contact influence created by mine detectors during normal use in detection operations are expressly prohibited. Self-deactivating mines with anti-handling devices that are also self-deactivating are expressly prohibited. Anti-personnel mines which are not detectable are expressly prohibited. All mine used or produced after 1 January 1997 shall incorporate a material or device that enables the mine to be detected by commonly-available mine detection equipment and provides a signal equivalent to at least 8 grams of iron in a coherent mass. All remotely-delivered mines shall be designed so that no more than 10% will fail to self-destruct within 30 days and have backup mechanisms such that fewer than 0.1% will function as mines after 120 days.

Protocol III (***Protocol on Prohibitions or Restrictions on the Use of Incendiary Weapons***) has the following provisions. It is prohibited to make the civilian population the object of attack by incendiary weapons. It is prohibited to make any military objective located within a concentration of civilians the object of attack by air-delivered incendiary weapons. It is prohibited to make any military objective located within a concentration of civilians the object of any incendiary attack except when such military objective is clearly separated from the concentration of civilians and all feasible precautions are taken to limit the incendiary effects to the military objective. It is prohibited to make forests or other kinds of plant cover the object of attack by incendiary weapons except when such natural elements are used to cover, conceal, or camouflage combatants or other military objectives. Tracers, illuminants, and smoke munitions are not considered to be incendiary weapons.

Protocol IV (***Protocol on Blinding Laser Weapons***) prohibits the employment of laser weapons specifically designed, as their sole combat function or as one of their combat functions, to cause permanent blindness to unenhanced vision. In the employment of laser systems, the Parties shall take all feasible precautions (including training) to avoid the incidence of permanent blindness to unenhanced vision. Blindness as the incidental or collateral effect of the legitimate military employment of laser systems, including laser systems used against optical equipment, is not covered by the prohibition of this Protocol. Permanent blindness means irreversible and uncorrectable loss of vision which is seriously disabling (corrected visual acuity of less than 20/200 Snellen measured using both eyes) with no prospect of recovery.

Note: the United States has not ratified either the protocol on incendiary weapons or the protocol on blinding weapons. The U. S. currently has a formal stated policy in place that prevents the U. S. from further development of blinding laser weapons. However, this could change with changing administrations. Furthermore, the various Judge Advocate Corps of the military services have unanimously concurred that laser blinding weapons are not in violation of prior international law and in fact are more humane than weapons designed to kill the intended targets. The author could describe at length the exact physiology and prognosis of laser eye injuries. Foveal damage is the most serious (usually resulting in clinical blindness) but is likely to affect only those few troops who are attempting to fire directly at the laser weapon carrier at the time the laser weapon is used. The much more likely extra-foveal injuries produce less serious long-term visual acuity reductions (nominally 20/40 or less) and the visual perception process tends over time to accommodate for the second small blind spot produced. Every eye has a blind spot (where the optic nerve enters the eye) that the perception process has learned to ignore. In short, the author believes the injuries produced by laser weapons are usually much less serious than popularly imagined or as argued by opponents of laser weapons. More than a few laser researchers have experienced blinding laser injuries. Most of these individuals have resumed their careers without needing white canes and dark glasses. Their injuries are handicapping but not completely incapacitating. The author knows of no knowledgeable individuals, including himself, who would prefer death to the injuries a typical laser weapon would produce. Such individuals undoubtedly exist, but the author has not met them. Many people might protest that they would rather die than lose their sight, but few people actually commit suicide when they suffer a vision-impairing accident or illness.

The International Committee of the Red Cross is the non-governmental agency that voices the strongest support for banning blinding weapons [260] and has been a driving force behind the entire Convention on Conventional Weapons. The ICRC is devoted among other things to halting warfare of all kinds, eliminating all weapons of war, and ending human suffering. These are all laudable goals. However, it appears that in the eyes of the ICRC, any weapon banned is one less weapon that needs to be banned, regardless of any priority based on degree of humaneness. Given the unlikelihood of eliminating all weapons and all conflicts at this point of human societal development, the author believes that mankind would be better served by emphasizing weapons that preserve life over those that take life, even if disability results. ***It is likely that the last word on laser blinding weapons has not yet been heard.***

APPENDIX M. POTENTIAL DISRUPTIVE TECHNOLOGIES

In the military arena we can consider any technology that has the potential for providing revolutionary new capabilities or quantum leap improvements in old capabilities to be a potential disruptive technology. The disruptive technology need not be developed initially for military applications. Commercial breakthroughs will become "militarized" at an exceeding rate in the future. Witness the fact that computer technology was initially driven by military needs (the first computers were used for cryptography, generation of ballistic tables for artillery, and calculation of nuclear weapon designs) yet today it is the consumer segment that is pushing microprocessor technology to ever-increasing performance.

The United States military forces are vulnerable to disruptive technologies, as are virtually all other military forces. Vulnerability to disruptive technologies is a transient process. It begins whenever an adversary develops or deploys a new capability first and ends when we respond by matching deployments of similar capability or deployment of an effective countermeasure capability. The duration of the "window of vulnerability" depends on our ability to respond effectively, which often depends on where we were positioned in the race to develop the disruptive technology. Our existing force structure, doctrine, and traditions may make it difficult for us to develop or exploit such technologies when given the opportunity. For example, consider an adversary's development of artificial intelligence for replacing pilots in aircraft with computers. This was discussed in an earlier section of this work. If the adversary exploits this technology, then that adversary can gain an aviation capability that is as far ahead of today's U. S. aircraft capability as the aluminum monoplanes of WWII were ahead of the wood-and-fabric biplanes of WWI. The U. S. is among the leaders in both aircraft and computer technologies. By all rights, the U. S. should be the first to develop pilotless (or at least remotely piloted) combat aircraft. However, not surprisingly, aviators dominate the U. S. aviation development communities. Few attempts to eliminate pilots (and thus the source of future military aviators) from combat aircraft are vigorously pursued. Because we are not aggressively pursuing our own development, we are offering an opening to potential adversaries, and may also be significantly lengthening the window of vulnerability that would result if an adversary pursued that opening.

In Table M-1 we list a number of potential disruptive technologies. The list is broken into those with relatively near-term potential (probable development and deployment timeframe is within the next 25 years) and longer-term potential (probable development time frame is at least 25-50 years or possibly much longer). In the remainder of this chapter we will discuss the potential military impact of each of these potential disruptive technologies. The technologies marked with an asterisk in Table M-1 have already been discussed in earlier sections and will not be discussed in depth at this time.

The reader should note that many of these disruptive technologies sound like science fiction. In truth since few of them are currently practical, they are science fiction. However, the reader is reminded that atomic weapons and nuclear submarines and space flight were all science fiction for decades before they became science fact (and military reality). None of the technologies listed below violate the basic laws of physics. A number are likely to become practical and well established within one or two decades. Most will be realized before the 21st Century is half over.

Table M-1. Potential Disruptive Technologies

*Artificial Intelligences
*Trans-Atmospheric Vehicles
*Directed Energy Weapons
*Terminally-Guided Ballistic Missiles
*Weather Control
Advanced Algorithms
Target Recognition, Identification, and Discrimination
Micro-Electromechanical Systems (MEMS)
Z-Plane Electronics
Scalable Neural Network Chips
Direct Mind-Computer Interfaces
Very Energetic Materials
Electromagnetic Launch
High Energy Density Power Supplies
Bionic Augmentation
Ultrastrong Fibers
High-Temperature Superconductors
Cold Fusion Power Supplies
Deep Diving Submarines
Quantum Computers
Passive Coherent Location
Ultrasensitive Magnetic Detectors
Ultrasensitive Gravitational Detectors
Active Element Conformal Array Antennas
Nanotechnology
Nanites
Genetically-Engineered/Cloned Warfighters
Fusion Power Plants
Nuclear Catalysts
Matter-Antimatter Reactors and Weapons
Tectonic Weapons
Gravity Control
"Warp" Drive
Psychic Weapons
Space Colonies

* Already discussed in earlier sections of this report

The discussion presented here will vary in depth and detail. The fields are too diverse for the author to describe everything to the same level of detail. In the same light, the list of potential disruptive technologies cannot be complete. The nature of technological change indicates that as many new radically new discoveries will be invented every 15-20 years as have been invented in all of prior history. [213],[214] One cannot even dream of all of the possibilities that will become reality.

Artificial Intelligences

Within the next 20 years computer systems will have computational and memory capabilities that exceed those of the human brain. Sometime thereafter, the software needed to implement true machine intelligences will be implemented. Even before that, "associate" systems or expert systems with the ability to handle uncertainty in inputs will find widespread use. Associates could eliminate the need for trained personnel in a number of functions including most non-criminal law, medical diagnostics and routine treatment, accounting, etc. Intelligent lay personnel or personnel trained only to operate the "associate" might perform many of the functions currently reserved for doctors, lawyers, or certified public accountants.

In the military, associates might find application in reducing battle and planning staffs. They could almost certainly replace warrant officers and senior non-commissioned officers currently needed to maintain complex electronic equipment. A moderately trained enlisted person could perform almost any maintenance or diagnostic task if he had an associate capable of using visual and audio inputs, and capable of asking and answering questions based on the data presented to it. We are currently experimenting with using teleconferencing to facilitate some such functions. Here we are merely replacing the living remote "expert" with a computer-based embodiment of that expert's training and experience.

The application of artificial intelligence (to unmanned aircraft) has been discussed in Chapter 4. Similar application to unmanned surface combat vehicles and undersea combat vehicles should be even easier than to aircraft. Several cultures have found that some of the most effective weapons employed human operators willing to sacrifice their lives to achieve victory. Artificial intelligence would permit kamikaze-like weapons to be deployed without the need to sacrifice the operator (and eliminating any possible last minute changes of heart on the operator's behalf).

Coupling such intelligent computers with robots made practical by advances in microelectromechanical systems will lead to entities with important military uses. For example, a multi-armed intelligent robot might be capable of performing damage control functions on ships (or even aircraft) that human sailors (aviators) could not perform. They could repair hull damage in flooding or even flooded compartments. They could fight fires without undue regard for heat, smoke, toxic gases, electrical malfunctions, etc. They could repair equipment in high radiation environments such as nuclear reactor containment vessels. They could operate in chemical or biological warfare environments (and perform critical decontamination functions) without need of special equipment. They would also be far superior to human soldiers in performing routine functions such as equipment maintenance, ordnance assembly and handling, and material transport.

Use of intelligent robots is likely to ultimately lead to development of true androids (intelligent anthropomorphic robots). Android soldiers could operate all existing military equipment, reducing if not eliminating the need for new equipment acquisitions. They would be capable of superhuman acts, would be difficult to kill or totally disable, would be unrelenting and fearless in the pursuit of their assigned objectives, could operate in environments hostile to human soldiers, and would almost certainly strike terror into the hearts of most human soldiers facing them. Android soldiers could lie buried under sand, soil, or even water for days while conducting ambushes. They would not need to be continually supplied with food or water, only ammunition. Hundreds of android paratroopers could be crowded into a transport aircraft capable of carrying only a few dozen human paratroopers. They could be transported to the theater of operations as bulk cargo. A single container ship might transport could transport hundreds of thousands. An army of millions of android soldiers could be maintained in an inactive state for a tiny fraction of what an army of thousands of human soldiers could be maintained. Training of android soldiers would be unnecessary – all needed skills could be loaded as software. Simply maintaining a force in being would cease to be a costly and facilities intensive endeavor. Clearly, artificial intelligence promises to be a truly disrupting technology.

Trans-Atmospheric Vehicles

Several countries are currently pursuing the development of trans-atmospheric vehicles (TAVs). This technology will alter the way humanity views not only intercontinental travel but also space travel. Space travel will become an intrinsic part of intercontinental travel. The mystique and aura of danger associated with rockets as intrinsic aspects of space travel will not be associated with a "space plane". As ordinary travelers experience space flight, the aura and mystique will disappear. More people will demand the ability to spend extended time in space. Space stations and space colonies are almost certain to result. TAVs will also open new possibilities in warfare by reducing reaction times and minimizing periods of aircraft vulnerability. They may also permit the global transport and debarkation of troops on time scales shorter than local forces can be redeployed to counter them. The military applications of trans-atmospheric vehicles have been discussed in Chapter 4.

Directed Energy Weapons

Weapons that kill at the speed of light have long been a staple of science fiction. However, the U. S. and some of its allies will soon field one or more weapons with just such a capability. Such weapons will be able to engage many dozens of threats per minute compared to a handful for missile-based weapons. Greatly increased speed or agility will provide only marginal benefits to targets. Reliance on saturation attacks will become more problematic for the attacker. On the other hand, the characteristics of directed energy weapons are such that it may be advantageous to the attacker to resurrect the concept of armor. An inch of stainless steel may utterly defeat a weapon designed to burn through 1/16" aluminum, yet impose only moderate and acceptable reductions in missile performance. In short, directed energy weapons will force military forces to rethink the entire way they do battle. They truly represent a disruptive technology. Directed energy weapons have been discussed in Chapter 6 and Appendix I.

Several technologies may permit applications of directed energy weapons to be realized. The first is the development of extremely compact electron particle accelerators for pumping free electron lasers. Almost all aspects of free electron laser weapons can be currently packaged into practical sizes except the electron accelerators. Compact accelerators will be moderately disruptive in their own right as they will facilitate a variety of nuclear medicine therapies that are currently limited by the high cost of accelerators. The second is the development of scalable, coherent array diode lasers. Solid-state diode lasers are compact, power efficient and cheap when purchase in large quantities. If independent diode lasers can be coupled to form single coherent apertures (in a fashion analogous to active phased-array radar transmitters – see Appendix E), then the powers necessary for weapons application can be obtained directly. If active phase control is part of this process, then the beam director (see Appendix I) might be eliminated as well. Another facilitating technology is the development of compact high-energy power supplies. These are discussed further in a later section in this appendix.

Terminally-Guided Ballistic Missiles

Ballistic missiles have always been a difficult threat to counter. Their long range and high velocity have made them almost impossible to kill. Even after 30 years of development, ballistic missile defense is still very much hit and miss. Strategic deception and target mobility have been the most important ways of defeating ballistic missiles to date. When ballistic missiles gain the ability to perform significant maneuvers, to identify and discriminate their targets from the background, and home in to hit moving targets, then they will have gained one more jump ahead of the missile defense designers. Such technology has already been demonstrated by the United States (in the Pershing II intermediate range nuclear missile) and is being developed by at least two technically competent potential adversaries. Terminally-guided ballistic missiles have been discussed in Chapter 4.

Weather Control

The ability to accurately forecast the weather has proven its military utility time and again. An additional ability to control the weather would clearly be a disruptive technology. Our growing knowledge of the forcing functions and responses that produce specific weather conditions will grant us the ability in the relatively near future to alter if not actually control the weather. We should be able to control small-scale weather phenomena within one or two decades. Control of large-scale phenomena such as typhoons will probably be possible before the middle of the 21st Century. The ability to control the weather for peaceful purposes implies an ability to control the weather for military purposes. The use of weather as a weapon has been discussed in Chapter 7.

Advanced Algorithms

The term "advanced algorithms" is a catchall for computer programs that do more than simply execute a deterministic set of instructions. Artificial intelligences as described above are clear examples of advanced algorithms, but many other forms are possible. Almost all advanced algorithms will involve some sort of intelligence.

Each form of advanced algorithm described here is essentially a separate disruptive technology. That is, they tend to be stand-alone accomplishments. A breakthrough or demonstration of one form of advanced algorithm does not imply that breakthroughs or demonstrations of other advanced algorithms will be forthcoming.

There are many activities that can be described as “advanced algorithms”. A few of the possible ones are described below. They include:

- **Self-organizing databases** – databases that automatically sort inputs into appropriate fields and is capable of finding all possible relationships between data elements, including those not pre-conceived by the programmers.
- **Natural language compilers** – programs that automatically translate natural language (e.g., English prose) instructions into compilable programs in a high-level programming language such as C++.
- **Reverse compilers** – programs that take existing executable computer programs (regardless of original source language) and generate source code in a specific high-level programming language. These programs facilitate reverse engineering of old codes and deciphering of acquired codes.
- **Automatic symbolic commenting programs** – programs that take undocumented (uncommented) source code programs, determine the higher level mathematical operations the source code programs perform, and generate comments using natural language and symbolic mathematics. These programs facilitate reverse engineering of old codes.
- **Direct manufacturing programs** – programs that can take a three-dimensional drawing package and generate programs to control numerical controlled machine tools and robots to automatically fabricate and assemble complex mechanical systems.
- **Integrated circuit board design programs** – programs that combine computer-aided design tools, performance simulation tools (such as SPICE), thermal analysis modeling, and reliability prediction tools into an integrated design environment. Such codes would permit designers to see all aspects of circuit performance (including steady-state response, transient response, heat generation and dissipation, and reliability) as each component is added to a complex electronic circuit board.
- **Evolutionary design programs** – programs that combine genetic algorithms and natural language inputs to evolve novel design solutions with significantly improved performance.
- **Serial-parallel partitioning programs** – programs that can take complicated numerical problems and automatically partition the problem into serial versus parallel processes and optimally allocate the computations between multiple processors.

Many others are undoubtedly possible. However, they are beyond the ability of the author to identify and address them at the present time.

Advanced algorithms are disrupting in that, in every instance, the developer will be able to solve highly complex problems or perform highly complex tasks without requiring significant human labor in achieving the results. Some of these advanced algorithms will undoubtedly be useful in addressing military problems or making military equipments. The previously unobtainable solutions or the remarkable reductions in equipment costs will be the disruptive influence. For example, if equipment design, development, and production costs can be reduced by an order of magnitude, then it becomes possible to consider procuring ten times as many units. The concomitant increase in military capability would clearly prove disruptive (not only to an adversary who must face the improved capability but also to our own forces who must adapt to the luxury of quantity as well as quality).

Target Recognition, Identification, and Discrimination

Automatic target recognition has been the focus of extensive study for thirty years. Automatic target recognition is the process of finding (without human viewer intervention) small targets in highly cluttered images having large fields of views. Except in limited applications, the target recognition problem has not yet been satisfactorily solved.[248] Target identification is the related process of determining the identity of a detected (and possibly hostile) target to a sufficient level of confidence that the target will be attacked or allowed to proceed unmolested. Decoy discrimination is the related process of determining whether a detected potential target is a real target or decoy intended to draw weapons away from real targets.

Future weapon systems desire the ability to prosecute multiple targets in short times. For example, a goal of current aircraft systems is the ability to generate 4 kills per sortie. This is not difficult to achieve if the targets are massed in tight formations or in convoys. However, it is almost impossible to achieve when targets are widely dispersed in pre-prepared positions and/or extensively camouflaged. Automatic target recognizers (ATRs) can facilitate high kill rates per sortie. Ideally they will be able to detect potential targets even when they are partially obscured by terrain or foliage and/or routinely camouflaged. ATRs can also facilitate the coverage of extremely large areas in small times, releasing the system operators to perform time critical functions such as flying the aircraft. The overload resulting from placing both target acquisition and piloting functions on the operator frequently degrades the ability to do both. Even if a separate weapon systems operator is provided, ATRs can in principle perform the target detection functions faster than that operator. Target recognition is limited to determining whether a detected object belongs to a militarily significant target class (e.g., a tank versus a small car or a truck). It does not guarantee that the target is hostile.

Target identification is performed by a combination of sensors and processing algorithms to provide reliable and robust classification of potential targets into specific military classes. Ideally, such systems would be able to discern friendly targets from hostile targets from neutral targets ((IFFN – Identification of Friend, Foe, or Neutral). In practice it is doubtful that any sensor system will ever be able to read the mind of the operator of a target to determine his true intent. For example, it will not be possible to unequivocally declare that the pilot of a friendly aircraft has secretly turned traitor and is attempting to carry out a hostile act (until that act has been initiated). Similarly, it is not possible to determine that the pilot of an aircraft belonging to a hostile air force is trying to defect rather than trying to carry out an attack. It is also not even possible to determine if the pilot of a hostile aircraft is actually going to attack or merely simulating an attack. Encounters of the latter kind occur all too frequently.

Target identification may be cooperative, non-cooperative, or semi-cooperative. Cooperative systems involve the targeting system interacting with the targeted system to elicit a specific response from the targeted system. For example, the targeting system may ask "Are you friendly?" via an encrypted message from a radio frequency interrogator and the target (if friendly it will be able to decode the interrogation) will reply "I am friendly!" via an encrypted message from a radio frequency transponder. Current cooperative interrogation-response IFFN systems may be jammed, they may be exploited, and they give erroneous results if a transponder malfunctions or is turned off. Non-cooperative systems make their determination of identity based solely on the data that can be obtained by their associated sensor systems. For example, a thermal imager may obtain a high resolution thermal image of the target which is subsequently processed by a image understanding and pattern recognition algorithms to identify the target. Current non-cooperative target recognition systems have not proven capable of providing sufficiently accurate identifications. Some targets are mis-classified; others are not able to be classified properly. Semi-cooperative systems involve the modification in distinct ways of observable characteristics (attributes that sensor systems can detect and measure) of friendly targets. For example, on D-Day in 1944, the aircraft were painted with highly visible black and white stripes. Semi-cooperative systems are usually only useful for limited periods of time. For example, the German Luftwaffe could have copied D-Day stripes within a few hours had it been to their advantage (they either decided it was not or just didn't think to do it).

Barring the pathological situations mentioned above, it is conceivable that appropriate sensors could unequivocally identify the type of target to such a degree that means, motive, and opportunity can be inferred to a degree sufficient to permit lawful use of lethal force in response. It is even more likely that such sensors could eliminate all but the most pathological examples. For example, a viable target identification system would have unequivocally identified the Iranian airbus that was shot down by the *USS Vincennes* as a commercial airliner (and not an F-14 using commercial airline IFF codes). A commercial airliner might be used in a kamikaze attack on a warship, but that situation is sufficiently pathological that launching a surface-to-air missile would have been unwarranted without considerable additional evidence. Identification of a target as being of the same model as those used by U. S. forces, even if the adversary possesses a limited quantity of that same model, would reduce the *a priori* probability of an attack to a low enough level that weapons launches should be prohibited, barring significant additional evidence to the contrary.

Decoys have reached a high degree of sophistication. Inflatable vehicle decoys can mimic the size, shape, color, texture, radar reflectivity, and thermal emission of real vehicles yet cost a thousand times less. An entire decoy tank army can be deployed for less than the cost of a single real tank. It is rumored that nine out of ten "tanks" destroyed by NATO air forces in the Kosovo conflict were decoys. The decoys were intentionally exposed to detection while the real tanks were kept hidden. Reentry vehicle decoys (called penetration aids) can be equally confusing to sensors and seekers associated with ballistic missile defense systems. An ICBM might carry 10 to 100 decoys for each reentry vehicle (nuclear warhead) carried. Without decoy discrimination 1000 interceptors might be required to guarantee destruction of the 10 warheads from a single MIRVed ICBM. Decoy discrimination is essential to guarantee that the real targets are identified and destroyed without excessive wastage of expensive weapons.

Micro-Electromechanical Systems (MEMS)

Micro-electromechanical systems (MEMS) [215] are a disruptive technology that is just beginning its disruptive run. Rotating wheel gyroscopes the size of a baseball are being replacing by vibrating quartz tuning forks the size of a paperclip. These may be shortly replaced by differential pendulum accelerometers the size of a printed lower-case letter etched into silicon. Micro-mirror arrays with each mirror capable of being independently positioned via electrostatic forces can modulate light beam and produce projection displays or simulate targets moving against backgrounds for imaging seeker testing. MEMS technology basically involves the ability to machine micron-sized mechanical parts out of silicon, quartz, and other materials using the lithography, photoresist, and etchant technologies developing for making integrated circuits.

Sensors of many different types can be envisioned. Chemical sensors based on changes in mass or conductivity produced by adsorbed species. Pressure sensors, strain gauges, temperature sensors, accelerometers, magnetic field sensors, electric field sensors, and electromagnetic radiation detectors, among others are possible. Some of these have been available and used for years. Actuators of different types can be envisioned. Any mechanism that can be constructed on a macroscopic scale (centimeters) using steel, aluminum, or brass can be fabricated at the microscopic scale (tenths of millimeters) in silicon, quartz, or other semiconductor material. Gears, racks and pinions, worm screws, pendulums, torsion bars, etc. can be microminiaturized. Coupled with integrated circuit electronics, almost anything might be fabricated at microscopic scales.

Future military applications of MEMS technologies might be highly interesting. For example, motors the size of a printed period might operate miniature robotic "insects" that could covertly infiltrate enemy positions in the manner of flies or roaches. Once there they may hide behind a baseboard or on the ceiling and "bug" enemy headquarters units using silicon sensor eyes or ears. Similar devices with small explosive charges might attack military bases in swarms, seek out critical electronic components (e.g., radios or computers), mechanical components (e.g., engines, generators, or even ordnance), or even people, and destroy or damage them. What sort of "insecticide" do you use on a swarm of explosive "bees"?

Z-Plane Electronics

Modern electronics is essentially two-dimensional. Processor chips may have several square centimeters of area, but the individual devices seldom penetrate more than a few tens of micrometers into the silicon wafers in which they are fabricated. Chips are interconnected at the edges. As a result, electronic circuits tend to be built on long, wide, yet thin circuit boards. These may be stacked one above the other in a card cage, but the resulting structure is still mostly air or unused circuit board. Z-plane electronics adds a third dimension to circuitry.

Ordinary electronics package their circuits on thin boards, z-plane electronics package theirs in compact cubes. Many benefits can derive from this. First, electronics can be made more resistant to shock, vibration, and acceleration. Large, thin boards are much more likely to flex or break under high g loadings than compact cubes. Second, total weight will be reduced as the supporting structure will be much smaller with z-plane electronics. Third, total volume will be dramatically reduced because the air spaces are removed. Fourth, highly parallel circuits are more naturally constructed in three dimensions. For example, staring focal plane array imagers need individual preamplifiers and storage buffers for each of tens of thousands of detector elements prior to multiplexing. This is a natural application of z-plane architecture.

Z-plane architecture has not yet become the norm for several reasons. First, electronic circuits generate heat that must be removed. Two-dimensional architecture can take advantage of flat design to conduct heat away from semiconductor devices in the z direction. However, it is possible to design conduction or convection cooling elements into 3-dimensional architectures. Second, current design tools and fabrication equipment is set up to do two-dimensional designs. Although development of three-dimensional tools and machines is a financial constraint on implementation, there is no fundamental barrier to such three-dimensional circuitry. Third, a mistake or flaw anywhere in a three-dimensional circuit may make it necessary to discard the entire circuit. In two-dimensional circuits, a failed component can be readily removed and replaced. This is more difficult in a three-dimensional design.

Scalable Neural Network Chips

Neural networks have revolutionized some forms of computation. However, at the present time, large neural networks (those capable of solving the more complex problems) must be simulated in conventional computers. This negates the parallelism inherent in neural networks which is one (but not the only one) of their attractive features. If neural network chips were available that could be scaled to arbitrary numbers of neurons and arbitrary numbers of synapses by directly connecting outputs from one chip to inputs of adjacent chips (as is done in array processors), then simulation could be avoided. Enormous gains in processing throughput could be achieved. A simulation requires thousands to millions of clock cycles to achieve what one or two clock cycles would achieve in a neural network chip.

Scalable chips would permit large neural nets with high throughput to be easily assembled. The resulting neural nets might be used to perform pattern recognition functions in support of automatic target identification. They might facilitate the computation of phase shift associated with conformal array antennas. They might also facilitate the implementation of large-scale content addressable memories and associative processors. Lacking scalable chip implementations, neural network applications have been predominantly hypothetical. Scalable chips will make neural networks practical in real systems.

Direct Mind-Computer Interfaces

Many science fiction writers have described life in a world where people are directly interfaced to their computers. The interfaces were occasionally audio-visual with computer-generated audio and video outputs (the latter displayed on a small handheld screen or on compact goggles) coupled with voice recognition for input. Such interfaces can be purchased today. In other instances, the computer was literally wired into one's brain with a plug and cable. Surgically implanted devices permit computer-generated signals to stimulate appropriate parts of the brain to provide "output" functions and to measure and interpret neural electrical signals to obtain "input" functions. Such interfaces are under study today and may become practical within a few years. Still other interfaces involved the equivalent of wireless transmission or telepathy. Wireless interconnection to the "plug" interface is possible with existing technology. Other work is examining the ability for limited communication directly to the brain with microwave signals. However, true telepathic interconnection is still in the realm of science fiction (if not actually fantasy). Interfaces associated with a "plug" promise to be highly disruptive in their own right, although telepathic interfaces would be even more disruptive should they occur first.

Military personnel with direct mind-computer interfaces would be capable of much faster response in any given situation. Recognition of a situation might be accelerated because the entire "big and little pictures" are directly input into the brain. This would negate the need to visually scan displays that in turn need to be manually generated by others (or at a minimum generated by a computer and output onto a video monitor). The input might be impressed on the brain in a fashion that guarantees better long-term memory and recall than is currently achieved with visual or audio input. The user would have instantaneous access to any of a number of computer-based decision aids. He would not be slowed by a need to input key data into separate programs. It is possible that such direct linkage might produce fewer errors such as hitting the wrong key. Finally, once a decision has been made, it is instantly communicated to the computer for immediate action. The operator no longer needs to take even a few seconds to push a button. Communication between individuals would be faster. One person wired to the network needs only to think a message for it to be sent to anyone else wired to the net. It may even be possible to multiplex many different inputs that are currently difficult to handle.

Since we do not have a complete understanding of conscious thought and neural function, such direct interfaces may open up possibilities we cannot even imagine at this time. Direct neural connections might facilitate training. It might be possible to convert computer data directly into stored memories. One might learn a language overnight by having the appropriate CD-ROM downloaded directly into human memory. Alternatively one might translate in real time by accessing a computer translation program running in a multitasking environment. One might learn how to fly a specific airplane or operate any weapon system without ever accessing real hardware or even virtual reality simulations of the hardware. Training might be shortened from months to mere days spent on technical details. When connected to a group, the knowledge of one individual might be able to be shared with everyone. In summary, it is possible that direct mind-computer interfacing could result in ten-fold reductions in required reaction times with ten-fold improvements in the quality of the decisions being made. The degree of coordination would also be strongly increased. Being connected to a group would almost be the equivalent of being able to read each other's minds in real time. It is not impossible that such a merger of thoughts and memories might result in the equivalent of a "superintelligence". If two brains are better than one, what is a network of tens or thousands or millions (all sharing thoughts and memories) equivalent to?

One fringe category of information warfare has been described as Gibson warfare [90] in honor of the science fiction writer William Gibson. In Gibson warfare, virtual reality entities fight in cyberspace yet produce consequences in real space. Direct connections between a network and the human brain of the form described above leads to a possibility that a cyberspace attack might be capable of permanently altering the connected human's mental processes or possibly even killing him. Gibson warfare would have left the realm of science fiction and become reality. Along these lines we commonly talk about one individual's mind being stronger than another's. In a merged-brain situation, would stronger individuals dominate weaker ones or would individual personalities disappear entirely? Would individual personalities reappear when the individuals disconnect from the network?

Very Energetic Materials

Current energetic materials (explosives and propellants) have energy contents that are in the range of 2 to 6.2 MJ/kg, detonation velocities between 4.8 and 9.2 km/s, and Chapman-Jouguet (C-J) pressures between 140 and 390 kbar. For comparison purposes, TNT has an energy content of 5.40 MJ/kg, a detonation velocity of 6.93 km/s, and a C-J pressure of 190 kbar, while HMX has an energy content of 6.19 MJ/kg, a detonation velocity of 9.11 km/s, and a C-J pressure of 387 kbar. Since modern delivery platforms usually impose weight constraints on any warhead, then the energy content is a direct measure of potential performance. The higher the energy content, the more energy can be delivered to a target by a warhead of specific weight. The detonation velocity and the C-J pressure can be related to the explosive quality of brisance (shattering ability). The higher the detonation velocity, the more energy contained in the explosive shock wave. The higher the C-J pressure (essentially the pressure of the detonated explosive products immediately after detonation), the more force can be applied to confining material structures. Ideally, the explosive community would like to find explosives with much higher values of all three parameters than are currently achieved.

The energy of many modern explosives is associated with nitrate or amino groups attached to organic backbones. There are other ways in which chemicals can store energy. For example, molecules have extra energy when molecular bonds are strained by bending more tightly than normal. For example, carbon atoms normally form tetrahedral bonded structures with an angle of 109.5° between any two atoms bonded to the carbon. However, the carbon atoms in cubane lie on the corners of a cube with three of the bonds forming 90° angles. Because of this excess energy in the strained bonds, cubane is much less stable than octane (having the same number of carbon atoms but with tetrahedral bonding). The potential nitrogen analog of cubane (octaazacubane – N_8) is roughly equally strained. It has the further advantage of being a potential one-product (gaseous nitrogen – a "hard" molecule from a mass acceleration perspective) explosive. Tetranitrotetraazacubane (four cubane carbons replaced by nitrogen atoms and four nitro groups bound to the remaining carbons) is predicted to have an energy content of roughly 7.8 MJ/kg, a detonation velocity of almost 10.4 km/s, and a C-J pressure of 540 kbar. [254] The compound tetrahedrane (four carbon atoms bound into a tetrahedron – each carbon bound to other three carbons) is even more highly strained than cubane. The compound dinitrodiazatetrahedrane is predicted to have an energy content of roughly 9.37 MJ/kg (more than 50% higher than HMX), a detonation velocity of 10.9 km/s, and a C-J pressure of 590 kbar. [254]

Another highly strained compound might be made by combining the pentanitrogen cation with an azide anion, to produce N_5N_3. [255] The pentanitrogen ion has a calculate heat of formation of 350 kcal/mole which corresponds to an energy content of 20.9 MJ/kg (of ion). The addition of the azide ion is expected to add perhaps another 70 kcal/mole (total heat of formation of approximately 420 kcal/mole). This is an estimate based on heats of formation of 64.4 kcal/mole for HN_3, 71.0 kcal/mole (per azide ion) for $Hg_2(N_3)_2$, 57.1 kcal/mole (per azide ion) for $Pb(N_3)_2$, and 73.8 kcal/mole for AgN_3. Thus, we would expect pentanitrogen azide to have an energy content of 15.7 MJ/kg.

It is likely that some of these highly strained compounds will be capable of mass production. What is not yet clear is whether they will be stable enough (i.e., insensitive enough to environmental conditions of heat, shock, etc.) to be usable as military explosives.

Other high energy density energetic materials might be formed from metal slurries such as powdered aluminum and water or powdered aluminum and concentrated hydrogen peroxide. "Slushes" made from combustible gases frozen into "snows" as they bubble through liquid oxygen can have very high energy content, although some of these materials are extremely sensitive. For example, a stoichiometric acetylene-oxygen slush has an energy content of 7.57 MJ/kg. This is considerable higher than HMX but not in the category of a super-energetic explosive. It is, nevertheless, one of the most energetic condensed phase explosives that has actually been synthesized. It is unfortunately extremely sensitive, and probably unusable for military purposes. However, it might make an excellent terrorist weapon as it can be improvised in the field.

It is clear that there is a possibility of using strained bonds, slurries, or other approaches to create super-energetic materials with energy contents that are considerably higher than that of TNT, perhaps as high as 20 MJ/kg. It is of great interest to know the maximum energy that a purposefully designed chemical explosive might be expected to achieve. The energy content of a hydrogen/oxygen explosive mixture is roughly 13.8 MJ/kg and is the most weight efficient explosive mixture known that involves simple molecules (that is one reason why hydrogen and oxygen are so often used as space launch rocket fuels). We have also seen that pentanitrogen azide might be as high as 16 MJ/kg. Super-energetic formulations may gain energy storage in the form of bond strain, but do so at the expense of requiring multiple heavy atoms per molecule. One electron volt of stored bond energy divided by the mass of a hydrogen atom is equivalent to 95.74 MJ/kg. Normal chemical bond energies are of the order of a few electron volts (ultraviolet photons with 5 eV energy can break bonds in almost any organic molecule), while the masses of the atoms forming the bonds are usually many times that of a hydrogen atom. Normal chain molecules have less than one bond per atom (e.g., a diatomic molecule has one bond divided between two atoms). So-called "single bonds", "double bonds", and "triple bonds" are counted as one bond each. Ring-like molecules have roughly one bond per atom. Molecules with interlocking rings (such as cubane) may have between one and one and a half bonds per atom. For a molecule with an average of 1.5 bonds per atom with an excess energy of 1 eV due to bond strain and an average atomic weight of 14 per atom (i.e., nitrogen) we calculate an energy content of only 9.1 MJ/kg.

If the total excess energy in the molecule greatly exceeds the energy of a single typical bond (of the order of 10 eV) then it is likely that thermal fluctuations will eventually lead to a conformation that favors spontaneous decomposition. For this reason it is doubtful that more than 2 eV excess energy per bond can be achieved in a material stable at room temperature. Thus, we might expect that 18 MJ/kg is a likely upper limit to what can be achieved. This is an estimate; the actual limit may be somewhat lower. If cryogenic storage (below liquid nitrogen temperatures, i.e., <77 K) were a practical option then this limit might be raised considerable. However, even if cryogenic storage were an option, materials with the ultrahigh bond strain still need to be identified.

If super-energetic (>15 MJ/kg) explosives can be synthesized with sufficient stability for safe handling, it would open up numerous possibilities. Warheads could be miniaturized while retaining the same explosive power. Only 350 kg of a super-energetic explosive would provide the destructive capability of 1000 kg of TNT. This would permit much smaller weapons to be built with performance equivalent to larger weapons. Alternatively, the yield of existing-sized weapons could be increased 3-fold. For example, a single 250-kg bomb would approach the destructive power of our largest bombs (1000 kg). Either way, the roughly 8000 kg bomb load of a single F/A-18F carrying advanced explosives would have 75% the destructive power of the bomb load of a B-52 carrying roughly 32000 kg of conventional explosive bombs.

Alternatively, the smaller warheads would permit considerably longer ranges or higher velocities to be achieved using airframes of comparable size to existing airframes. If warhead weight were kept the same, the lethal radius of the warhead would be almost doubled. The kill radius of a fragmentation warhead is nominally proportional to the square root of explosive yield. If the higher explosive yield per unit mass was accompanied by higher detonation velocities (this is almost certain to occur given the higher energy densities), the shattering effect (brisance) of warheads would be considerably enhanced. This might improve the capabilities of deep-penetration warheads to destroy hardened buried targets.

If used as propellants, such super-energetic materials could lead to three-fold reductions in motor size (for comparable payload weights) or three-fold increases in missile range (for comparable motor weights). Coupling super-energetic propellants with super-energetic explosive warheads might permit total missile size to be reduced 10-fold with no loss in capability (smaller warheads permit smaller motors to propel them at the same speed over the same distance). An AEGIS cruiser could conceivably carry 500 or more missiles in the same space as each current 64-cell VLS launcher module.

Electromagnetic Launch

Electromagnetic launch is actually a family of closely related technologies all of whom use magnetic forces to accelerate "projectiles". Specifically, we may talk about electromagnetic guns, electromagnetic aircraft launch, and electromagnetic satellite launch (or mass launchers). Each of these three uses different configurations and different forces so we must discuss them separately.

Electromagnetic guns use magnetic forces to accelerate small projectiles to extreme velocities. A high velocity v gives even a small mass m a significant kinetic energy T according to the equation

$$T = 0.5mv^2$$

A 1-kg mass accelerated to 10000 m/s velocity has a kinetic energy of 50 MJ. This is equivalent to the energy released by detonating 11.9 kg of TNT. Electromagnetic guns can use the projectile's kinetic energy to kill large targets without the need of explosive warheads.

The most common form of electromagnetic gun being pursued is the rail gun. In a rail gun, a conductive projectile completes a short circuit between two conductive guide rails. When a large current is discharged through the circuit, the current in the projectile interacts with the magnetic field to produce a Lorentz force on the projectile, accelerating it down the length of the guide rails. The accelerating force is proportional to the square of the current that can be forced through the rails.

One advantage of electromagnetic guns is that they use relatively lightweight projectiles, without warheads or separate propellant. Thus, many more projectiles can be carried than can conventional shells. The guns themselves may be lighter, may be more rapidly aimable, and may have higher rates of fires. These potential advantages may or may not be realized in a practical design. For example, the rate of fire will depend on how fast the gun's energy storage mechanism can be recharged and this will be a function of the size of the prime power supply. One undeniable advantage is the short time of flight resulting from the high velocity. This facilitates aiming (target lead angle and range drop are both dramatically reduced) and reduces the probability that an adversary can get off a killing shot.

Electromagnetic launch of aircraft basically replaces the steam-driven cylinder of current catapult systems with a linear induction motor. Simple magnetic attraction of unlike poles and repulsion of like poles provides the motive force. After injection into the motor section by hydraulic or compressed air ram, a shuttle made of permanent magnets is accelerated by a conventional electromagnet stator assembly. The stator elements change polarity as the shuttle passes to maintain a constant force.

Electromagnetic launch of aircraft has a number of potential benefits over conventional steam catapults. First and foremost, the need for a large steam plant is eliminated. This saves considerable space and weight on a ship. It also makes gas turbine or diesel prime movers more attractive relative to nuclear power than they were when a steam plant was required. Elimination of the steam plant also allows much lower infrared and acoustic signatures to be achieved. It also eliminates a major consumer of maintenance man-hours resulting in reduced life-cycle cost. Second, it would facilitate the use of aircraft on somewhat smaller ships. The length and width of launch and recovery areas are determined by the g-loadings limits and size characteristics of the aircraft to be handled and are only minimally influenced by the launch (and recovery) mechanisms. Thus launch and recovery dictate the minimum deck area of an aircraft carrier. However, a considerable fraction of the size is determined by the need to have a large number of aircraft on deck. Because electromagnetic launch systems would likely consume less below deck volume of a ship, more aircraft could be kept in the hangar deck, rather than on the flight deck. Smaller aircraft carriers, with their accompanying significant construction cost savings (as well as operational cost savings), might mean that more aircraft carriers could be procured.

Electromagnetic launch is also more amenable to producing higher launch accelerations than steam catapults. The length of a catapult L required to accelerate an aircraft to a velocity v with an acceleration a is given by the equation

$$L = v^2/a$$

When the navy transitions entirely to unmanned aircraft (capable of higher launch accelerations), then electromagnetic launch will permit the same airspeeds to be achieved in shorter flight decks (with further cost savings in construction).

Electromagnetic launch can also be adapted to smaller carriers with smaller air wings. For example, ships the size of the current helicopter carriers (LHD and LHA) could incorporate catapult launch for their Harrier aircraft without sacrificing too much volume. Electromagnetic launch coupled with vertical landing would reduce many of the penalties currently paid in range and payload by short take-off/vertical landing (STOVL) aircraft and make them much more attractive. Assume the STOVL aircraft can tolerate the same launch accelerations as a conventional aircraft. If the STOVL aircraft can save 90% of the range penalty paid for near-vertical take-off by being catapult launched at 75 knots (compared to a nominal 150 knots for a conventional aircraft catapult launch), then the STOVL catapult needs to be only 25% of the length of the conventional catapult.

Electromagnetic launch of spacecraft might involve a combination of levitation and acceleration using the Meissner effect (the exclusion of magnetic fields from superconductors). The payload is carried by a carrier vehicle that is at least partially constructed from superconducting materials. A dc magnetic field levitates the carrier to eliminate frictional losses. The launch mechanism may or may not be partially evacuated to reduce aerodynamic drag. This mechanism is composed of a number of coils through each of which a high current can be discharged. Initially one coil is energized behind the carrier, producing a strong field gradient at the superconductor. The difference in magnetic pressure on each side of the superconductor produces the acceleration. As the carrier passes each coil current is discharged through the coil to continue the acceleration. Once the carrier and payload have reached orbital velocity, the carrier might continue into orbit and use orbital maneuvering thrusters to deliver the payload to a precise destination. The carrier can then return to the launch site by reentering similar to the space shuttle. Alternatively, the carrier could immediately eject its payload (to continue into orbit) and then be decelerated by additional coils whose current pulses are delivered just before the carrier passes them.

Electromagnetic spacecraft launchers will be very large. If we assume an orbital velocity of 8000 m/s and a maximum launch acceleration of 10,000 gees (roughly 50% of a typical gun projectile acceleration – good spacecraft designs can accommodate this level of acceleration), then the launcher must be 650 meters long. This is large but many bridges have longer spans. To launch payloads at a man-tolerable 3 gees, would require a launcher roughly 2200 km long. This is not practical. However, for a launcher with a maximum(?) practical(?) length of the order of 50 km, the launch acceleration could be reduced to roughly 130 gees (high, but most satellite systems could be designed to withstand such launch transients).

Electromagnetic launch of spacecraft offers significant potential to change humanity's view of space. Once initial construction costs are paid for, the cost of launching a payload into space will be little more than the cost of the electricity. If widespread fusion power or solar power is available, then this cost might be negligible. Many systems concepts have fallen by the way simply because it cost too much to place them in orbit. Another benefit is the ability to launch payloads at a rapid pace. Theoretically, a new payload could be launched as rapidly as the energy storage system could be recharged (seconds to minutes). Payload handling would probably limit launches to no more than a few per hour. This is to be contrasted with days to weeks between launches today. This means that even a massive project can be lifted to orbit in a few days or weeks rather than years (as the GPS system required or the Space Station is expected to require). The rapid launch pace will also impact the logistics of anti-satellite warfare. If an inventory of spare satellites is maintained on the ground, it is conceivable to have a replacement satellite on orbit within a single orbit time of the discovery of any satellite's destruction. Launch reliability and safety should also go up significantly. The electromagnetic launcher is more akin to a light rail system than to the Space Shuttle.

Although electromagnetic launch by itself is not practical for launching manned spacecraft into orbit, it may replace the first stage of existing systems. At 3 gees acceleration the 50-km long launcher could accelerate a manned spacecraft to roughly 1200 m/s velocity. This is fast enough that a scramjet engine could begin to operate efficiently or a single conventional liquid-fueled rocket stage could continue boosting the spacecraft into orbit. Elimination of the largest (booster) stage would have an enormous impact on cost as well as on safety and reliability. With low-cost, high reliability, and acceptable safety, it will be possible for anyone with a reason to go into space to be able to do so. Industrial processes that are better performed in space, will be (as opposed to still being expensive research projects today). Space tourism may be profitable. Without a doubt, the door will be opened to the colonization of space.

High Energy Density Power Supplies

Many potential military systems require extremely compact, high energy density power supplies to be practical. For example, low-energy directed energy weapons (laser dazzlers) require approximately 1 kW average prime power and run times of at least an hour (preferably tens of hours) to be practical in some man-portable infantry applications. If lead-acid or nickel-cadmium batteries were to be used, the minimum-sized battery alone would weigh roughly 40 kg (far too heavy to for an infantryman to carry). See Table M-2. [216] Even if lithium-sulfur dioxide batteries were used the minimal battery would weigh an excessive 5 kg. It would require a battery with an energy storage density of the order of 5 MJ/kg and a power density of the order of 1 kW/kg to make this and other applications truly practical.

Paths to realize the magic 5 MJ/kg @ 1 kW/kg performance levels have not yet been identified. However, there are a number of potential approaches. Batteries have not yet been proven incapable of achieving the desired performance. The energy storage efficiency of some battery systems is adequate, but the power density required has not. However, new battery materials are being developed are being developed all the time. Supercapacitors are charge storage devices that are capable of withstanding high internal field strengths. Energy storage efficiency

Table M-2. Characteristics of current power storage devices.

MATERIAL	ENERGY STORAGE EFFICIENCY WEIGHT	VOLUME	POWER DENSITY
Lead Acid Battery	0.1 MJ/kg	0.3 MJ/l	<50 W/kg
Nickel-Cadmium Battery	0.05-0.1 MJ/kg	0.1-0.2 MJ/l	30-150 W/kg
Lithium-Sulfur Dioxide Battery	1 MJ/kg	2 MJ/l	220 W/kg
Lithium-Thionyl Chloride Battery	2.0-5.5 MJ/kg	4-11 MJ/l	< 100 W/kg
High Explosive Generator	3-5 MJ/kg	3-5 MJ/l	3-5 x 10^5 MW/kg

in a supercapacitor will scale as the square of the internal field strength achievable. A quick estimate shows that 5 MJ/l can be achieved at field strengths of 10^9 V/m. This value is only one order of magnitude lower than the typical fields experienced by outer shell electrons in atoms. Thus, it is possible that supercapacitors may approach but not achieve the desired efficiencies. Hydrogen-oxygen fuel cells represent a third possible avenue of approach. The chemical energy stored in hydrogen (125 MJ/kg H_2) is more than adequate. However, the overhead associated with hydrogen storage and with the fuel cell itself has to date prevented them from reaching the desired performance. Cold fusion, although a long-shot candidate, is still a possibility because of the enormous energy efficiency associated with fusion.

If power supplies with the required 5 MJ/kg @ 1 kW/kg characteristics can be achieved, then many military devices may become practical. In the introduction to this section we mentioned the possibility for handheld directed energy weapons. Another application lies in the area of bionic augmentation (discussed in the next section). An average human being may expend roughly 3000 Calories (12.6 MJ) per day. Running can consume 300 Calories per hour (350 W). A 5 kg power supply with the "magic" characteristics above could provide 10 times the power consumed by running for a period of over 7 hours. Thus, it might be capable of powering a set of bionic legs running much faster than a human for a large fraction of a day. Other applications of high energy density power supplies include active sensors such as radars on remote platforms including satellites and electrically propelled miniature air, ground, and subsurface vehicles.

"Bionic" Augmentation

Medical science is at the verge of creating prosthetics with functionality comparable to the original "organ" and that are controlled by direct nervous connections. Artificial legs, hands, and arms have reached a level of maturity that it is difficult to label their possessors as "disabled". Within a few years we will have functional artificial eyes, ears, and noses as well as fully dexterous artificial limbs.

It takes no great leap of imagination to envision artificial limbs with built-in weaponry. Built in guns would be more accurate (pointing would not have to account for how the weapon were being held) and incapable of being lost in close quarters combat. An artificial limb could also contain “built-in” computer and communications equipment. Mechanical muscles could be made stronger than biological ones and would be less susceptible to fatigue or minor injury. Artificial eyes could incorporate low-light level or thermal infrared imaging capabilities (or both). Artificial organs could be developed that enhanced human healing capabilities. For example, blood gases and electrolytes can be monitored and altered to provide optimum performance. When bleeding is detected extra levels of platelets and/or clotting factors could be injected into the bloodstream. Glucose or plasma could be injected into the bloodstream if deficiencies due to excessive exertion for long periods without adequate refreshment and rehydration were detected. Performance might be enhanced by injecting drugs (such as stimulants, tranquilizers, or painkillers, as determined by circumstances) or by providing biofeedback control of physiological functions.

The benefits of bionic augmentation might be such that professional soldiers (voluntarily or otherwise, depending on the culture) would routinely undergo surgery to replace perfectly good organs with superior prosthetics. If one first-rate military power institutes this practice, could others refrain and place themselves at distinct disadvantages. There are deep cultural implications in this. The “branding” that would accompany bionic augmentation might cause an even deeper divide between the military and the civilian population than currently exists. The whole concept of civilian control of the military might be challenged.

If bionic mutilation is not an option because of these cultural limitations, then bionic augmentation in the form of mechanical exoskeletons or power suits remains an option. All of the bionic advantages described above can be provided without any need for sacrifice of limbs or organs. The powered battle armor that is a staple of science fiction lacks only high energy density power supplies to be practical today.

Ultrastrong Fibers

Many applications require materials much stronger and lighter than ordinary metals. These applications are now turning to composite materials using fibers (for strength) embedded in a matrix (to minimize fiber motion and wear). The strength of these composites depends on the strength of the fibers. Strong fibers are also being woven into fabric to provide strength and flexibility. Among the commonly used fibers are glasses (as in Fiberglas), synthetic polymers (such as Kevlar), and carbon (graphite), the latter being perhaps the best currently available. Carbon fibers have tensile strengths of about 5 GPa at densities of about 2.25 g/cm^3 (compared to 3 GPa at 7.9 g/cm^3 for steel). However, new and much stronger fibers are being developed. One of those being seriously studied is spider silk (dragline fibers) with strengths considerably greater than Kevlar. Current work is aimed at producing spider dragline silk from the milk of genetically altered goats. Unlike ordinary silk, which can be mass-produced by cultivating silkworms, spiders cannot be similarly grown in quantities and harvested like the silkworm cocoons. Until a viable source of spider silk becomes available, Kevlar and carbon are the primary fiber materials.

However, the most promising candidate appears to be fibers made from carbon nanotubes. A carbon nanotube is a tubelike stucture made entirely from carbon bonded in interlocking "benzene" rings. Nanotubes are close relatives of buckyballs. Buckyballs are a novel form of carbon derived from the original molecule to be discovered, C_{60} or buckminsterfullerene. In buckminsterfullerene each carbon has one double bond and two single bonds to other carbon atoms forming a spherical shell of carbon that looks like the geodesic dome designed by Buckminster Fuller, hence the name. Other "buckyball" molecules have been found that have other shapes, including tubes. The entire nanotube is essentially a single molecule. Mechanically breaking such a fiber would be the equivalent of mechanically pulling a molecule into halves. In fact, a large number of extra strong chemical bonds would have to be broken in order to break a nanotube. Recent measurements indicate that the tensile strength of an individual nanotube is 30-50 GPa. [217] Theoretical estimates of the strength are as high as 200 GPa. Thus, there is reason to believe that strengths of 100 GPa or higher may be achieved as the technology matures. The density of a nanotube should be somewhat less than the density of graphite. Thus, nanotube composites could have ten times the strength of steel at one-fifth the density. The same materials would be several times stronger than equivalent pieces made from Kevlar or graphite fibers.

The applications of super-strong fibers are numerous. Body armor could be made lighter and capable of stopping even larger projectiles than currently possible. Super-lightweight airframes would make possible routine human-powered flight as well as ultra-long endurance air vehicles. Main battle tanks could have increased armor protections while shedding half of their current weight (or more). Armor would once again become a practical design consideration for ships and aircraft. Airframes capable of pulling 50-100 g maneuvers while fully loaded are another possibility. These super-agile airframes would be almost impossible to shoot down with interceptor missiles. Even though missile airframes could be made even more agile using the same materials, improvements in seeker technology would almost certainly also be required.

The added strength with reduced weight would also allow extremely large structures to become practical. Suspension bridges with 100-km clear spans become thinkable. So too, do very large space structures. In the 1970s NASA determined that space colony platforms enclosing volumes of the order of 1000 km^3 were feasible using steel construction materials. [218] The primary limitation was the cost of lifting the huge weight of metal into orbit. Using super-strong fiber materials, comparable structures could be built with weights that are a few percent of the comparable steel structures. Finally, nanotube fibers might actually make the "Space Elevator" possible. [219] The "Space Elevator" is a cable drawn elevator with one end attached to the Earth at the Equator and the other end in geosynchronous orbit. Satellites could be launched merely by pulling them up in the elevator car. Detailed design studies have indicated that a material of 60-70 GPa strength is required to make such an elevator a practical reality. A practical space elevator could eliminate the launch costs that make many projects impractical. For example, large space stations, space colonies, space-based ballistic missile defense, and interplanetary manned spacecraft are among the projects that a space elevator could make cost effective.

High-Temperature Superconductors

The use of superconductivity has long been negated by the need to cool the materials to temperatures below the liquefaction point of hydrogen (and more preferably to liquid helium temperatures, i.e., 4.2K). [220] However, in the past two decades considerable progress has been made in extending the temperature at which superconductors can operate. Current capabilities allow operation at temperatures somewhat above the temperature of liquid nitrogen (77K). Since cryogenic coolers can readily achieve this latter temperature, a number of new military applications are being considered. Unfortunately, these high-temperature materials are essentially ceramics and lack flexibility. Current research is aimed at incorporating these materials into bendable "wire" that can be used to fabricate practical electric devices. It may be several years before such "wire" is available at reasonable cost. Furthermore, cryogenic coolers are costly, have reliability limitations, and can only cool relatively small devices. Thus, further improvements in high temperature operation are desired. When the limit is extended to roughly 200 K, temperatures which relatively inexpensive and reliable thermoelectric coolers can achieve, then a vast array of additional applications will become practical. When the limit is extended above room temperature, then normal-conducting devices and circuits will almost certainly become obsolete.

Among the devices and technologies that will benefit from high temperature superconductors we must include:

- **Low power consumption electronics** (superconducting interconnects remove one of the sources of power dissipation in electronic circuits).
- **Ultracompact high-power motors** (superconducting magnets will not overheat as easily as conventional electromagnets).
- **Higher power microwave devices**
- **Superconducting detector systems** (superconducting junctions make excellent broadband – infrared through microwave – detectors). Their current use is limited because of the need for excessive cooling.
- **SQUID seekers and imagers** – supersensitive magnetic detectors can be fabricated into large arrays if cooling were not required. Such arrays could be processed to provide directional and spatial shape information about any magnetic object. This would permit discrimination of targets from clutter and allow their use in weapon delivery applications.
- **Electromagnetic launch** – a superconducting linear motor would consume considerably less prime power than a conventional motor.
- **Ultra-high-speed rail transportation** – numerous designs exist for superconducting levitation rail systems. The cost of cooling low-temperature superconductors has been one factor in their failure to gain acceptance on a wide scale.
- **Magnetic bearings** can permit nearly frictionless suspension of large objects. Very high rotational velocities and/or energies would be permitted.

Many other applications will undoubtedly appear when this technology matures.

Cold Fusion Power Supplies

The announcement of the discovery of "cold fusion" in March 1989 prompted an immediate disavowal by the scientific community. [221] Some of this was due to the "press conference" approach used in the announcement, some was due to perceived unwarranted speculation on the part of the discoverers, and some was due to the outsider effect (how could a pair of chemists discover a physical phenomena that physicists have been unable to discover). Despite the almost complete rejection of the phenomena of the scientific mainstream, the basic claim of excess energy generation was never disproved. Instead, the "fringe" community that continued to investigate the phenomena has proven the existence of excess energy beyond any reasonable doubt. A theoretical understanding of the phenomenon continues to elude scientists.

The lack of theoretical understanding does not preclude practical applications. Superconductivity was discovered five decades before the Bardeen-Cooper-Schrieffer (BCS) theory was proposed.[222] X-rays were being used in hospitals three decades before their origins in atomic transitions could be explained by the quantum theory. Even without an underlying theory, it should be possible to develop practical power supplies based on the cold fusion effect.

Given that the excess energy effect does not require enormous volumes of material to manifest itself, it appears that one of the first applications would be in compact, moderate-power, generation systems (comparable to turbine engines or fuel cells). This would make "non-nuclear" (i.e. non-fission) submarines possible with all of the advantages of nuclear power, but none of the disadvantages. This would revolutionize undersea warfare. The lack of nuclear disadvantages would drive most surface ships to adopt cold fusion power as their prime movers. This would eliminate one of the current vulnerabilities associated with the need for frequent underway refueling.

Safe power plants would also be available for satellites and spacecraft. If megawatt powers were available on satellites without the threat of a plutonium radiothermal generator or a nuclear power reactor occasionally crashing back to earth, then radar imaging satellites could proliferate. Electrical power could be made available to remote regions with considerably less logistics burden (gallons of deuterium oxide compared to tens of thousands of gallon of motor fuel). The availability of megawatts powers from compact and safe reactors would make it possible to build truly mobile directed energy weapons, including directed energy weapons on spacecraft. Undoubtedly, hundreds of other uses would be manifest long before large-scale fusion powerplants for commercial electricity generation were ever built.

Deep Diving Submarines

Improvements in materials and improvements in automation and artificial intelligence (permitting reduced manning or even elimination of manning) will permit truly deep diving submarines – submarines capable of operating at depths of several thousand meters or more. Such submarines may have considerably smaller pressure hulls with more of the submarine at ambient pressure. This will reduce the truly vulnerable area of the submarine. It will also facilitate the use of multiple outer hulls. In addition, many of the features needed to harden the ship against pressures ten to one hundred times greater than those currently faced will provide added resistance to conventional weapons when at shallow depths. Depth charges, torpedoes, direct-hit shaped charge weapons, and even nuclear depth charges (at reasonable standoff ranges) may not provide kills. Such submarines will also be able to dive deeper than any current antisubmarine weapons are capable of functioning. As a result, if they are capable of detecting an attack early enough to permit them to reach the depths before the weapons can catch them, they will be essentially invulnerable. Even if they are unable to dive deeper than the attacking weapons, they may be able to reach the ocean bottom, where increased reverberation and topographic features will make it easier to confuse both active and passive sonar seekers.

Deep diving submarines will be harder to detect. Intervening thermal layers can completely reflect acoustic emissions from the submarine. The normal refractive ducting present in acoustic propagation in the ocean will make it difficult for a deep submarine to be detected by any shallow platform. Acoustic waves emitted in the deep sound channel will tend to stay in the deep sound channel. The ability to dive deep permits submarines to access more of the ocean bottoms. A submarine lying "dead" on the ocean bottom will be almost impossible to detect except with the most sophisticated side scan sonar systems. If a deep submarine can remain undetected until a battle group passes overhead, then it has a good chance of rising rapidly to the surface, prosecuting a successful attack, and returning to the safety of the depths before a counterattack can be mounted.

Development of deep diving submarines will almost certainly be accompanied by development of weapons (torpedoes) capable of functioning in those depths. In this case, the submarine may never need to leave the depths in order to prosecute an attack. Torpedoes appearing out of nowhere will be difficult to defend against. Given the potential for submarine maneuvers at depth before beginning the final attack phase will give the surface forces little or no information with which to find and attack the submarine. In essence, deep diving submarines will create a truly three-dimensional underwater battlespace, in which surface ships, aircraft, and shallow diving submarines will be inadequately prepared to compete.

Quantum Computers

In ordinary computers numbers are represented in binary notation as strings of "bits" (bistable operating states of electronic circuits that can represent a "0" or a "1" – 5 bits can be used to represent any integer between 0 and $2^5-1 = 31$). The computer solves problems by instructing selected strings of bits to be altered according to a selected sequence of operations called a program. In a **quantum computer** bits are replaced by qubits (quantum bits) which can represent a "0" or a "1" or any value in between or more than one value simultaneously. Five qubits can represent all of the numbers between 0 and 31 simultaneously. This property is a manifestation of quantum mechanical uncertainty. Another property of qubits is that each qubit is weakly coupled to every qubit – another manifestation of quantum mechanics. Changing one qubit has the ability to subtly change every other qubit. External forces can be applied to each qubit to cause it to have higher or lower probability of representing a "1" or a "0". The program in a quantum computer is the sequence of applications of these external forces to selected groups of qubits.

Many elements of the quantum computer "art" are in hand today. In 1981 Richard Feynman proved theoretically that any physical system could be simulated on a quantum computer of appropriate size. [223] This means that the technology should be applicable to solving virtually any physical (vice metaphysical) problem of interest. By 1994, Peter Schor at AT&T Laboratories established the first algorithm (program) suitable for processing by quantum computer. [224] In March 2000 a team at Los Alamos National Laboratory showed that a quantum computer could be built using the spins of atomic nuclei composing a molecule. The spins could be altered by magnetic resonance using frequency-tuned pulses of radio frequency radiation. In August 2000 a group at IBM actually solved a simple problem, order finding, using a quantum computer. At labs around the world, researchers are looking at using nuclear spins, superconducting junctions, acoustically trapped electrons, and quantum dots (microscopic bumps on silicon) to implement ever larger, faster, and more stable quantum computers.

The power of a quantum computer is that all possible solutions to a problem are calculated simultaneously. A 32-bit microprocessor operating at 1000 MHz can perform approximately 32 billion one-bit operations every second. A 32-qubit quantum computer operating at 1000 MHz will perform the equivalent of 4.3 billion billion one-bit operations every second (8 orders of magnitude higher). Quantum computers with only 25 to 30 qubits should be capable of solving a significant number of problems. They will be capable of solving those problems in only a few machine cycles (microseconds?). Quantum computers with hundreds of qubits will likely be capable of solving any problem we can currently think of. The enormous problem solving capacity of quantum computers will make them as revolutionary to computing today as the microprocessor was to computing in the 1980's.

The most obvious and possibly the first practical application of quantum computers will be in the area of cryptography. Schor's algorithm [224] can be used to factor large numbers, a key step in breaking many of the most sophisticated encryption schemes.[224] These encryption schemes are based on keys which are the products of very large prime numbers. If the two prime number factors can be determined, the encrypted messages can be decoded. Virtually every code based on pseudorandom sequences will be rapidly decipherable. It is possible that all encryption techniques (except one-time pads) will be rapidly decipherable and secret communication will no longer be possible. If this transpires, it may be impossible to achieve strategic surprise. Diplomatic communications will be forced to bypass all forms of electronic communication.

Network-centric operations will be severely affected. If encryption technology becomes rapidly decipherable, then our intelligence data, commands, and all other forms of communication will become rapidly transparent to almost every adversary. Your adversaries will know everything communicated over the network almost as quickly as you know about it or transmit it.

Even commonly used systems will be vulnerable to exploitation. Low probability of intercept radars and communication links employ spread spectrum transmission and pulse compression reception. The pseudorandom noise-like spread spectrum techniques are readily amenable to detection by quantum computers. All possible pseudorandom sequences can be analyzed in parallel by a quantum computer. Any receiver with a quantum computer can obtain the full processing gain of the intended receiver (that knows the pseudorandom sequence). Thus, low probability of intercept devices using spread spectrum techniques will cease being low probability of intercept. This will make it even harder to implement highly stealthy platforms. Such platforms will be forced to operate under complete communications silence and will have to employ purely passive sensors.

Passive Coherent Location

It has been observed since the earliest days of radio, that an object moving between a transmitter and a receiver will cause interference. Observation of such interference ultimately led to the invention of radar. The weak radio signal which has "reflected" off of the moving object will interfere with the radio signal traveling on a direct path between the transmitter and receiver. The phenomenon is closely related to multipath in conventional radar systems. In truth, it is multipath in a bistatic radar geometry. The interference manifests itself as a roughly sinusoidal amplitude modulation that begins with low amplitudes and high frequencies and gradually grows in amplitude whiles its frequency decreases. The amplitude grows to a maximum at some minimum frequency and then the process reverses with the amplitude decreasing while the modulation frequency increases until the amplitude becomes so small and/or the frequency so large that the effect seems to disappear. After the interference damps out, the reflected signal may appear as a faint ghost image.

Passive coherent location uses the simultaneous detection and processing of such interference from at least transmitters at different locations. The phase and frequency of the modulation produced by a single moving target using a single transmitter depends on the position of the target relative to the transmitter and receiver, on the target velocity, and on the carrier frequency of the radio signal (which is known). Measurement of the interference parameters from three transmitters permits determination of the target position and velocity (in three dimensions if the transmitter and receiver locations are precisely known; or in two dimensions if the transmitter locations are not known;). Measurement of the parameters from a larger number of transmitters can permit tracking in three dimensions using transmitters of unknown locations.

Passive coherent location systems can be implemented using existing transmitters (such as television or radio stations) and ubiquitous receivers (such as home television sets) with a telephone or radio system to communicate the time at which maximum interference is observed. Maximum interference will occur when the target passes closest to the line of sight between the transmitter and the receiver. A distributed network of such receivers with a central processing center to correlate interference reports can provide coarse tracking of airborne targets. Improved performance can be obtained by performing more detailed analysis of the signals from each receiver and transmitting this data to the correlation center. A single receiving station analyzing the signals from multiple distributed transmitters can eliminate the need for networking. Even better performance can be achieved if dedicated transmitters are used to transmit ideal waveforms and dedicated receivers are used to detect and analyze those waveforms. In this last instance we have evolved to a netted multistatic radar system. It still falls within the classification of passive coherent location because the receivers are not collocated with the transmitters.

A variety of passive coherent systems are being pursued. The Lockheed Martin Silent Sentry system uses a sophisticated receiver to process signals from multiple radio and television transmitters.[249] China appears to be developing a similar system.[250] Russia has offered to sell a radar barrier system called Struna-1 which uses a linear array of bistatic radars operating in a forward scatter geometry. Other systems are under active investigation.

The interest in passive coherent location stems from its counterstealth potential. Most air defense radars currently operate in a monostatic or backscatter geometry (receiver co-located with the transmitter). Stealth design attempts to minimize scattering of radar radiation back towards the radar. One consequence of minimizing backscatter is that radar reflection in other geometries (including forward scattering) is at worst minimally reduced and may in fact be considerably enhanced. Thus, passive coherent location systems (which use forward scattering geometries) will be minimally affected by current designs for stealth. Both stealthy and non-stealthy targets will be detected, tracked, and engaged. Any attempt to design for additional stealth in the forward scattering geometry will probably cause increased scattering in the backscatter geometry (which is unacceptable). Thus, passive coherent location systems may turn the U. S. commitment to stealth platforms into an expensive liability. If stealth no longer guarantees survivability, then U. S. forces will be severely disrupted. Tactics and doctrine must change. Missions may have to go unaddressed. Added casualties must be anticipated.

Ultrasensitive Magnetic Detectors

The development of superconducting quantum interference devices (SQUIDs) has led to the development of ultrasensitive magnetometers and compact magnetic gradiometers. SQUID-based magnetometers can be three to four orders of magnitude more sensitive than fluxgate magnetometers. Since the dipole components of magnetic fields (including magnetic anomalies) fall off with the inverse power of range, three orders of magnitude improvement in sensitivity implies a potential increase in detection range of one order of magnitude (10X), assuming the detection range is not limited by clutter. Because SQUIDs are basically two-dimensional devices (they are similar in size to microprocessor chips), whereas fluxgates are three-dimensional (they are typically longer than they are wide), SQUID magnetometers can be considerably smaller than fluxgate magnetometers with comparable flux areas. The recent advances in high-temperature superconductivity permits the manufacture of SQUIDs that operate at liquid nitrogen temperatures (77K) rather than liquid helium temperatures (4 K). Liquid nitrogen temperature SQUIDs can be employed in numerous military applications whereas liquid helium temperature SQUIDs cannot.

One obvious application is to replace fluxgate magnetometers in traditional magnetic anomaly detectors. In this application, there may be reductions in size achievable. However, the increase in sensitivity may not translate into increased detection range because clutter (magnetic rocks and debris from sunken vessels) often limits detection range. The use of gradient magnetometers may improve this somewhat.

Another potential application is in mines or fixed-position sensors. Since a mine or a fixed-position sensor (such as an element of a grid of sensors) looks for time-dependent variations of the magnetic field (not space-dependent variations), they will be relative insensitive to the clutter that limits airborne magnetic anomaly detectors. A ten-fold increase in range allows magnetic detectors to play a role in deeper-water mines similar to CAPTOR. Alternatively, the increased sensitivity would require any magnetic-silencing (used to defeat magnetic influence mines) to be performed an order of magnitude better than currently required. Ships that are deemed adequately silenced today would trigger mines with more sensitive magnetic detectors.

The magnetic field changes produced by current vessels could be detected at ranges of the order of 10 km. Thus, SQUID magnetometers could be incorporated into a grid with 10-20 km element spacing covering a large area with a management number of elements. For example, a region 200 km by 1000 km (roughly the size of the entire Persian Gulf) could be covered with only 500-2000 sensor elements. Virtually any vessel larger than a corvette, surface or subsurface, could be continuously tracked anywhere within the sensor system. The application to submarine tracking (of even the quietest electric drive boats) would make it virtually impossible for submarines to operate in littoral waters without detection and subsequent attack.

Ultrasensitive magnetic sensor might also be useful in seeker applications. Although non-ferromagnetic aluminum, titanium, and composites dominate aircraft construction materials, virtually every aircraft, even stealth aircraft must have some magnetic materials or magnetic field producing components, such as electrical generators. These fields might be detectable at distances of the order of a kilometer or more. If a fire direction system can get a missile close to a target, if only by chance, then a gradient magnetometer might be able to guide that missile with sufficient accuracy to hit the target, even if it had virtually no radar, infrared, visual, or acoustic signature.

Ultrasensitive Gravitational Detectors

All objects have gravitational fields that are proportional to their mass. Furthermore, we currently know of no way to mask or alter those gravitational fields. Sensitive gravitational field detectors could provide robust target detection capabilities. Gravity gradiometers would further enhance detection sensitivity. They might be very useful in detecting stealth aircraft. Any mass detected flying between the sensor and the sky must be a target of interest. It is conceivable that an array of ultrasensitive gravitational detectors would prove to be the ultimate in counterstealth systems. Gravitational anomalies might also be useful in detecting submerged or buried objects. Cavities such as tunnels or buried bunkers might also be detectable.

Active Element Conformal Array Antennas

Phased array antennas for radars (see Appendix E) are usually considered to be superior to conventional reflector antennas. On many platforms, normal antenna sizes (including those of current phased array antennas) are severely limited. Weight will limit the size of antennas placed on masts. Clear area will limit the size in aircraft applications. Available superstructure area limits the size of phased array antennas mounted on many surface ships. On some platforms, the maximum power available is limited by the powers that available power amplifiers can produce. Active element conformal array antennas can significantly increase available antenna size by allowing the phased array to be wrapped around the entire skin of the platform, rather than being localized to the restricted space available to a flat rigid array. In addition, maximum power is determined not by amplifier size but by the number of active elements in the array. Adding more elements will increase the available transmit power as well as increase the size of the antenna.

This not only decreases beamwidth and improves angular resolution, it also increases the antenna gain, which further enhances target detection and tracking ability.

There are several critical technology elements in implementing active element conformal array antennas. These include development of the active elements, development of sensors for determining the exact position in space of each element, and a processor for calculating the phase shifts needed to form the beam for each choice of beam direction and set of antenna element locations. The active elements must include amplifiers, phase shifters, and duplexers. The position sensors may yield absolute position measurements, although it is sufficient to provide position measurements relative only to the neighboring array elements. The processor must calculate the phase of each antenna element relative to a hypothetical wavefront propagating in the desired direction. This is not difficult but it is computationally intense.

Conformal array antennas would find immediate use in fire control radars on aircraft. Aperture size in these systems is limited by the fuselage diameter. Placing the antenna elements along the wings and fuselage would increase the field of view of these radars as well as improving angular resolution and increasing antenna gain (increasing useful range). Target detection radars on helicopters are another potential application. Placing the array in the rotating helicopter blades would eliminate current weight constraints (they are usually mounted on a mast above the main radar) and provide more than an order of magnitude improvement in target location accuracy. Conformal array antennas may also make it possible to implement viable ballistic missile defense radars on board surface ships. The nominal requirement of 3×10^6 W-m^2 (defined in the ABM treaty as the threshold for ABM radars) can be met by a radar with a 10 m x 30 m antenna transmitting 10 kW average power.[201] Conformal arrays are also tailor-made for unmanned vehicle applications. Size and weight are critical in such application. There is seldom as much space available as desired. By using conformal array antennas, the maximum available area can be used and weight allocated for antenna structure can be kept to a minimum.

Nanotechnology

Nanotechnology [228]-[230] is engineering and manufacturing at the molecular level. In its ultimate form, devices of all kinds would be built atom by atom using machines called assemblers. An assembler would act according to a program and construct new devices by following that program to assemble the entire device one atom at a time using atoms from a pool of elemental resource materials. In this respect, an assembler is an extrapolation from a robotic assembly line that follows instructions from a program and constructs a car (or other object) one part at a time using parts drawn from inventory. With an assembler in operation, macroscopic devices would appear to literally grow from a stream of raw materials. Assemblers would obviously revolutionize manufacturing. A flexible assembler would be capable of making anything from a mass of raw materials, just by changing its program. It would be the “replicator” of Star Trek fame.

Work on producing an assembler is taking several approaches. In one approach, atomic force microprobes are used to position atoms one at a time on the surface of a substrate. Get the first desired atom and place it onto the substrate. Get the next desired atom and place it on the substrate at the desired position relative to the first atom, and so on, until the finished product is assembled. Any sort of possible molecular structure could be built in this fashion.

Another approach recognizes that specialized assemblers already exist in nature in the form of ribosomes. A ribosome is a complex molecule that reads the "program" encoded in a strand of RNA and builds the encoded protein, one amino acid at a time. It is possible that artificial ribosomes could build other molecular structures using different basic building blocks. This work is still in its infancy.

It is hypothesized that macroscopic nanotechnology will revolutionize the world almost overnight, <u>when</u> the breakthrough occurs (i.e., a programmable assembler is perfected). Designs for nanoproducts and programs to produce them are already being generated in advance of the existence of the first assembler. Once produced, the first assembler will produce other assemblers. The existing designs and programs produced by others will immediately be adapted to the new assembler. The development process might grow factorially.

Nanotechnology can involve micro-machines fabricating macroscopic objects. It could also involve the fabrication of molecular-sized machines. This aspect of nanotechnology can be thought of as the extrapolation of micro-electromechanical systems (MEMS) technology from the microscopic scale to the molecular scale. Some structures have been made possible by the discovery of buckyballs. Buckyballs are a novel form of carbon derived from the original molecule to be discovered, C_{60} or buckminsterfullerene. In buckminsterfullerene each carbon has one double bond and two single bonds to other carbon atoms forming a spherical shell of carbon that looks like the geodesic dome designed by Buckminster Fuller, hence the name. Other "buckyball" molecules have been found that assume other shapes, including bowls and tubes. Addition of atoms other than carbon permits an unlimited variety of molecular shapes to be generated. Gears, shafts, bearings, tubes, vessels, etc. have already been designed from single complex molecules. Current investigations are looking at how macroscopic devices might be translated to the molecular level and how they would be powered. Robots the size of protein molecules might ultimately result from this work.

Much current effort is being spent on creating special nanoscale materials.[252] For example, the electrical properties of small particles of metals as well as small particles of insulators have been found to be strongly dependent on the size of the particles. Production of uniform nanoscale materials is expected to result in new electronic devices and in new chemical catalysts.

Another aspect of nanotechnology research is focusing on molecular switches.[252] Any entity that is capable of maintaining either of two distinct states and is capable of transitioning between those states given an appropriate stimulus can for a binary logic device. Several different kinds of nanoscale molecules have been found to exhibit two molecular configurations that can be externally selected based on the presence or absence of additional electrons. It may prove possible to create computers using these molecules. Given that these switches may be smaller than 10 nm and the scale of current computer switches is several times greater than 180 nm (the current lithographic linewidth achievable), it is clear that these molecular computer technologies offer the potential for major advances in computer packaging. They might extend Moore's Law for another 8 to 12 doubling times (15 to 20 years).

In the author's opinion, practical nanotechnology assemblers are at least several decades away. He will say the same about practical nanoscale machines. These will have the biggest impact and will be truly disruptive when they occur. The development and employment of special nanomaterials is occurring as the author writes. However, similar materials advances are made all the time and are not likely to be disruptive. Even though the development of practical nanoscale molecular switches is also likely in the next decade, the author cannot consider them disruptive either. The capabilities they will enable are evolutionary and predicted by Moore's Law. They will merely provide new and different mechanisms (adding to a sizable list of other possibilities) to overcome the technological limits that will likely prevent CMOS transistor technology from sustaining Moore's Law more than a few more doubling times into the future. It is assemblers and nanomachines that provide the disruptive potential to nanotechnology.

Nanites

The term "nanites" was popularized by "Evolution", an episode of Star Trek: The Next Generation [231] in which self-reproducing, robotic microbes employing nanotechnology [228] evolve intelligence. The term is loosely used today to describe any form of robotic microbe (reproducing or not; intelligent or not). The simplest form of nanite (a deterministically programmed, non-reproducing robotic microbe) is perhaps more described using Drexler's term "assembler".

Nanites might revolutionize medicine [232]. They could move throughout the body repairing damage to cell tissues, recognizing and killing cancer cells or pathogenic organisms, destroying and recycling harmful proteins or other toxins, and even diagnose and repair damage to the body's DNA. In short, they might make it possible to live forever (barring accidents). Short of this goal, they might regrow damaged organs, speed the knitting of broken bones, and clean arteries of built up cholesterol plaques, significantly extending human lifetimes.

Nanites could also be used as weapons, especially reproducing nanites. A nanite might do the opposite of one or more of the functions above, speeding death. They could convert normal proteins into toxic proteins. Consider a nanite that selectively produced botulinum toxin. A single nanite might be able to kill an individual within hours. Nanites might be able to convert normal proteins into the infectious kind – called prions – that cause Creutzfeldt-Jakob disease (the human version of bovine spongiform encephalopathy – mad cow disease). They could be made to be immune to normal biological defenses. They might be the ultimate strategic "biological" weapon. Conversely, nanites might be the only mechanism for curing any of the spongiform encephalopathies by selectively destroying the harmful prions. They could act as "universal" antidotes to nerve agents by recognizing and destroying any cholinesterase inhibitor that was not natural to the body. They could easily be made to act as antidotes to specific toxins such as botulinum.

Nanites might also act to degrade or damage the equipment of an adversary. For example, a single nanite that converted plastic insulation into conducting graphite would create a short circuit in an electronics system in a short period of time. Many such nanites would make virtually all electronics useless. Nanites might be used to turn petroleum supplies into worthless goo, alter the transparency of optical materials, or reduce the strength of structural materials. Anything a nanotechnology “assembler” might be able to make, a “nanite” might be able to unmake. The military implications are obvious.

Most importantly, nanites could fight other nanites. If the adversary introduced a toxin-producing nanite, we could program another nanite to either destroy the toxin or program that nanite to disassemble the toxin-producing nanite. If the adversary introduced nanites that turned gasoline into tar, another nanite might be used to turn the tar back into gasoline or to alter the mechanism of the adversary so that it no longer attacked gasoline. Once nanite technology become available to one side, it is essential that the other side quickly develops similar technology or it will be defeated (or worse).

Genetically-Engineered/Cloned Warfighters

One of the public fears associated with genetic engineering is the potential for creating “superhumans”. Mammals have already been successfully cloned. It is only moral (and governmental) restraint on the part of researchers that has prevented any publicized cloning of human beings. With the deciphering of the human genome (recently transcribed but not yet fully understood), genetic engineers will be in a position to alter any aspect of human genetics. In a few years it will be possible to select genes that lead to:

- increased size and strength,
- improved disease resistance,
- increased ability to repair internal tissue damage,
- increased tolerance of pain,
- increased brain size,
- faster reaction times,
- improved vision (higher acuity, improved field of view, or improved low light sensitivity),
- decreased sensitivity to heat or cold,
- ability to breathe effectively at high altitudes (say 10,000 m without an oxygen mask), etc.,
- increased willingness to follow orders,
- increased aggressiveness, and
- decreased survival instinct

It might also be possible to incorporate capabilities found in other animals, such as:

- gills to breath underwater,
- webbed feet and hands to facilitate swimming,
- sensitivity to magnetic fields,
- sensitivity to electric fields,
- the ability to detect heat emissions from targets,
- the ability to generate electric shocks,
- the ability to produce and deliver deadly toxins,
- the ability to regenerate lost limbs or digits, or

- the ability to alter skin coloration to match the background.

If a number of these genes are inserted into a single individual it is possible to create a much-improved potential soldier. Cloning that individual to make thousands of copies could produce an army of super-soldiers.

The ramifications of such a capability have formed the theses of dozens of science fiction novels. Needless to say considerable public debate should occur before such an endeavor is even attempted. However, no amount of debate or legislation will stop an unscrupulous group or nation from attempting to clone superwarriors. The question that arises, is what is to be done when it occurs? Will such individuals be considered humans or animals or something different? Will society accept the use of such individuals in suicidal situations? After a conflict has ended what will the status be of the victorious clone-warriors? What will be the status of the vanquished clone-warriors? Should they be exterminated? Can they be integrated into a peaceful society? These are not easy questions to answer.

It seems unlikely that any amount of genetic engineering will make it possible for complete adult humans to be grown in periods of weeks or months, although it is likely that development could be speeded up significantly. Even with shortened development times it would likely take a decade after initial conception for any super-soldier to be useful. It is only this which has prevented the author from labeling this technology as a near-term risk. It is possible that such super-soldier projects could begin in earnest within a few years.

Fusion Power Plants

Whether they are based on cold fusion, magnetic confinement (tokamaks), or inertial confinement (laser implosion), fusion power will almost certainly become practical before the end of the 21st Century. With magnetic confinement and inertial confinement, the proof of principle demonstrations will be attempted before 2010. After that, power production is just a matter of "engineering" (despite the fact this is extremely complicated engineering) and power plant construction. After Fermi had demonstrated that his Chicago nuclear pile could sustain a chain reaction, there was no longer any serious doubt that either the atomic bomb or nuclear power plants would eventually be constructed. The same will be true for fusion power after the "energy breakeven" experiments are completed.

Fusion power will essentially consume deuterium and produce helium. There is enough deuterium in the oceans (roughly 2×10^{17} kg) to produce all of the world's energy needs for the next 40 billion years (at current energy consumption rates – roughly 4×10^{20} J/yr). Deuterium is available everywhere to anyone with access to electricity. The cost of generating electricity will become limited primarily by maintenance of production and distribution equipment, not by the cost of fuel. This should make energy extremely cheap, although it will never so abundant as to be free. It might cause governments to consider whether power generation should be government provided rather than provided by commercial concerns. If power generation were nationalized, it might prove cheaper not to charge directly per kW-hr consumed but to take the operating costs out general taxation revenues. Energy consumers might not have to pay fees proportional to the actual amount of energy they consumed, but proportional to the value of the goods they produced or the income they earned.

Fusion power will make it practical to provide unlimited amounts of power to even the remotest locations. No longer will fuel supplies and logistics be major considerations in reactor siting. One metric ton (one cubic meter) of deuterium will supply nearly 22 billion kilowatt-hours of electricity. This is equivalent to the annual energy output of a 2.5 gigawatt powerplant. Fusion reactors will necessarily be large if they are based on either magnetic confinement or inertial confinement principles. The huge capital investments required to build even a low-power output powerplant will suggest that higher-power plants (greater than tens of gigawatts) rather than lower-power plants (comparable to modern nuclear or fossil-fuel-fired plants) be built. Since even a low-power plant will probably be physically large, mobile platforms such as surface ships and submarine are unlikely to use them. Fission reactors are likely to remain the power source for naval vessels. However, the large concentration of power available from a large powerplant may make it possible to build large directed energy weapons. Laser or high-power microwave missile defenses might be facilitated by the development of fusion power.

Nuclear Catalysts

A number of years ago there was considerable interest in the possibility that muons could act as catalysts for nuclear fusion.[233] Unfortunately, the short lifetime of muons (2.2 μsec) has precluded their practical use. A catalyst facilitates a reaction (usually by lowering a potential barrier to the reaction) but is not consumed by the reaction. It may be temporarily used by one step in a complex process, but it must be regenerated in a later step. Because it is not consumed, a small amount of catalyst can cause an enormous amount of reactants to be transformed into products. In essence, neutrons are catalysts for nuclear fission in fissionable nuclides. More general nuclear catalysts, if they can be found, might make it easy to perform any number of energetically favorable nuclear reactions. These could include nuclear fusion or fission or transmutation.

With catalysts, it may be possible to achieve fission chain reactions or fusion reactions without the necessity for large masses of reactants. With fission catalysts, nuclear weapons could be scaled to any yield, including yields of only a few kilograms, and using correspondingly smaller quantities of fissionable material and reduced "fallout". Nuclear explosives could be considered (or reconsidered) for many applications where full-scale nuclear weapons were considered overkill or too "dirty". These include antisubmarine warfare, air defense, and hardened target destruction. The U. S. deployed nuclear weapons for these purposes at some point in its history but later removed them from the inventory.

Efficiency of fission is also likely to improve. A typical atomic bomb requires roughly 50 kilograms of Uranium-235 to form a critical mass [134], but a Nagasaki-sized 20 kiloton yield is produced by fission of only one kilogram of uranium. If a catalyst improved efficiency ten-fold, then the amount of fissionable material required to make an explosive device of a given size could be reduced ten-fold. The implication on the potential for nations (or terrorist groups) to acquire nuclear weapons is obvious. A single reactor that could provide material for one bomb per year can now provide material for ten. Alternatively, theft of a quantity of fissionable material that is not militarily significant today, might provide enough material to make one or two bombs. Catalysts might also make it possible to make nuclear explosives out of low-enrichment reactor-grade nuclear fuels.

Nuclear catalysts might also provide the "philosopher's stone" of ancient alchemy. For example, the "decay" of Pb^{204} into Li^7 and Au^{197} is energetically allowed, but is not observed in practice. A nuclear catalyst might make this reaction practical, literally permitting one to turn large quantities of lead into gold. Obviously, such an occurrence would make gold a relatively "worthless" metal, and ruin any economy that was still based on a gold standard. Military applications might include in situ alteration of the properties of materials, such as turning semiconducting silicon into conducting iron via fusion (and consequently destroying electronic systems) or causing fissionable materials in adversary weapons to explode by catalytically reducing the necessary critical mass below the mass of material that is present.

Matter-Antimatter Reactors and Weapons

The annihilation of matter and antimatter theoretically offers the most efficient conversion of mass into energy. For example, complete fission of 1 kg of U-235 releases 19.6 kilotons of yield. Complete annihilation of 1 kg of matter-antimatter releases 21.4 megatons of energy. The techniques being developed for magnetic confinement fusion power generation may also prove useful in the control, containment, and controlled annihilation of antimatter.

To date no natural terrestrial sources of antimatter have been found (nor are they likely to be found). In interstellar space there is considerable antimatter interspersed with more abundant ordinary matter. It is possible that an interstellar spacecraft could harvest this antimatter as a fuel source. It is also possible, but unlikely, that large clusters of antimatter (such as asteroids or planets) might be found elsewhere in the galaxy. Barring such unlikely natural sources, it is unlikely that matter-antimatter reactors will ever be primary energy sources in terrestrial applications. They will always consume more prime energy than they can produce. The antimatter must be created from conventional energy sources through nuclear pair production. Thus, matter-antimatter reactors will only be practical in applications where immense energies must be produced from relatively compact and lightweight reactors and fuels and the energy inefficiency associated with production of the antimatter can be balanced by the other benefits. Military vessels, interplanetary spacecraft, and energy weapons are likely candidates for using matter-antimatter reactors.

One reality must be faced. If matter and antimatter can be harnessed for power generation, it will be trivial to arrange their use in super explosive-weapons. Matter-antimatter annihilation is the most efficient form of conversion of mass into energy. Annihilation of one kilogram of matter-antimatter will yield 9×10^{16} Joules = 21 megatons (compared to only 3.4×10^{14} J = 81 kilotons for fusion of 1 kg of deuterium-tritium). The enormously powerful "photon torpedoes" of Star Trek will have become reality, for these science fiction devices have been declared to be missiles with matter-antimatter warheads. One medium-sized (e.g., 1000-kg) "photon torpedo" could release energy greater than the total yield producible by every nuclear warhead ever built. Uncontrolled annihilation is so much easier to arrange than controlled annihilation, that it is almost certain that the development of "photon torpedoes" will precede development of matter-antimatter power reactors by a decade or more.

Tectonic Weapons

It is a well-known phenomenon that the detonation of large underground nuclear explosions will trigger smaller earthquakes on nearby faults for days after the explosion.[225] In fact, underground detonation sites are chosen to have an absence of nearby large faults with rapid stress buildup. Studies of earthquakes at the Nevada Test Site [132] indicate that a nuclear explosion can affect the release of the energy in faults if any part of the fault passes within a distance R (in meters) of a nuclear explosion of yield W (in kilotons) where

$$R = 300\ W^{1/3}.$$

For reasonable nuclear weapons sizes, the effective distances are less than a few kilometers. However, it should be noted that none of the Nevada Test Site faults are classified as major earthquake-producing faults.

Recently two Russian nuclear scientists (identified only as Bekhterev and Krivoshlykov) at the Snezhinsk Nuclear Research Center (formerly known as Chelyabinsk-70) have announced that nuclear explosions may be used to reduce the possibility of earthquakes.[226] They claim that strong earthquakes were much fewer in the 1960's to 1980's, when underground nuclear tests were conducted with great frequency. Supposedly the nuclear explosions tended to reduce the accumulated tensions in the earth's crust.

Other mechanisms have been discovered that affect seismicity in local regions. The building of dams and the filling of their reservoirs are known to produce changes in local earthquake patterns. One acre-foot of water weighs more than 1200 tons and large reservoirs routinely store millions of acre-feet of water. Depletion of underground water and oil & gas reservoirs through pumping (fluid depletion) or injection of fluids into underground reservoirs (such as oil field pressurization) can produce similar alterations in local seismic activity. The removal of substantial amounts of rock through mining and quarrying also influences local seismic activity. [227]

As seismologists develop better understanding of tectonic forces, the properties of geological materials, and the subsurface structure of a region, they will ultimately be able to diagnose the buildup of stress and forecast its release. A genuine ability to predict earthquakes coupled with an ability to inject large amounts of additional energy into a system or the modification of external stresses may permit a certain degree of control over earthquakes, especially in their precise location, their precise timing, and their severity.

Any ability to control or even partially direct the forces associated with large earthquakes has obvious potential use as a weapon. It is doubtful that an adversary could ever initiate an earthquake in an arbitrary location at an arbitrary time. However, they might be able to increase the severity or modify the area of damaging effects by "fiddling with the system" in some fashion. A few nuclear devices might be clandestinely inserted (under the guise of mining or oil drilling) at specific locations around a major fault that is predicted to rupture in the near future. Detonation of the devices might then permit premature triggering of the earthquake and possibly magnify the amount of energy that would be released by causing a larger segment of fault or a nearby collateral fault to rupture. Such premature triggering might also be timed to occur at the time most critical in the target nation's preparations for the upcoming disaster and magnify the total damage achieved (for example damaging many of the equipment and facilities being constructed to facilitate disaster relief).

It might be difficult to directly affect earthquake faults in an adversary's territory. However, earthquakes themselves need not be the weapons. An adversary might be able to initiate vertical movements on undersea faults (either in their own coastal waters or in international waters and create enormous tsunamis that could then cross an ocean and devastate the coasts of an adversary. If several smaller movements were simultaneously triggered at different locations, a "phased array" effect could make it possible to concentrate the tsunami effects on some coasts and ameliorate them on others.

A nuclear explosion that immediately triggered an earthquake at the same point might be very difficult to detect and identify. Test ban treaty monitoring systems use both the shape and location of seismic signals to identify clandestine underground explosions. A nuclear explosion does not have the same characteristics as an earthquake. Explosions generate mostly compressional (P) waves, while earthquakes invariably generate more shear (S) waves than P waves (although there is always some P wave component). S and P waves travel at different velocities and are easily distinguished. Underground explosions cannot be hidden by triggering them when an earthquake occurs elsewhere. The monitoring stations can determine the location of origin of each seismic signal component. However, if the explosion and the earthquake occur simultaneously at the same point, the nuclear characteristics may be lost in the true seismic signal. Thus, the target country might never know that it had been attacked.

Finally, the ability to predict the timing of future earthquakes can be militarily useful in itself. For example, consider a prediction ability that lets it be known that a major (magnitude 8 or above) earthquake will occur on a specific fault in a specific narrow time frame (a few days). This prediction might come from computer modeling or from observation of identifiable earthquake precursors (many are currently being studied but none are yet reliable). However, any prediction of major disaster would cause national (if not international) attention to be focused on the disaster site. If the U. S. were the site of the impending disaster, an adversary could take advantage of the reduced external attention to prepare for any sort of military activity without drawing the same level of U. S. response it would have earlier. Once the disaster occurs, national attention, and in all likelihood, the military would be involved in disaster relief. This provides an excellent opportunity for direct attack by the prepared adversary. If the U. S. were the disaster area then the adversary could conduct other military operations (such as invasion of a neighbor) without the usual level of external intervention. Many U. S. forces would be co-opted for disaster relief. Strategic airlift, medical forces, and engineering units would all be committed directly to disaster relief. Some of these units would in all likelihood be withdrawn from overseas to augment CONUS-based units.

Gravity Control

The likely development of a viable quantum theory of gravity (or more properly a "theory of everything") some time within the next few decades will almost certainly be followed the development of technologies for the practical manipulation of gravitational forces and fields. By this the author does not imply the development of anti-gravity devices. These will most likely not be permitted by the theory, although recent discoveries concerning the expansion of the universe indicate that gravity may not be the invariable quantity it has always been believed to be. However, the generation and use of gravitational waves almost certainly will be permitted by any acceptable theory. A viable theory may also pave the way for the creation and manipulation of miniature black holes.

Small black holes (mass $< 10^{15}$ g) have been predicted by Hawking and others. These black holes are presumed to radiate energy (Hawking radiation) with a rate of emission that increases inversely with the mass of the black hole. As a consequence they might be useful as powerful explosives. On the other hand, it is possible to place a strong electric charge on a relatively stable, small black hole, thereby making it possible to control its motion by powerful electric and magnetic fields. A black hole oscillator would generate intense gravitational radiation. An array of such oscillators could be focused to produce devastating field strengths at remote locations anywhere in space. Earthquakes made to order would be "easily" produced. The solid earth provides minimal "shielding" effects to gravitational radiation. Such oscillators could also be used for one-way strategic communications to any point on earth (even deeply buried facilities or deeply submerged submarines) from a single location.

Gravitational collapse (gravitic) weapons (weapons in which mass is injected into a small black hole) could be created with enormous potential yields. Nuclear fission is only 0.1% efficient in converting mass into energy (efficiency = mc^2 (of energy out)/mc^2 (of mass in)); nuclear fusion is only 0.4% efficient. However, calculations have shown that gravitational collapse might be as high as 35-40% efficient in producing energy out per unit mass input. Only matter-antimatter annihilation is more efficient in converting mass into energy. For each kilogram of gravitic fuel mass, 8 megatons of yield would result (compared to 80 kilotons for the fusion of 1 kg of deuterium-tritium fuel). Weapons of fantastic size (gigatons) might be constructed.

"Warp" Drive

The same "theory of everything" that makes gravity control thinkable may pave the way for the development of "warp" drive or faster-than-light travel. Reputable scientists are now beginning to discuss the possibility of time travel and travel at equivalent speeds faster than light. The conditions currently believed to be required are beyond our technological abilities for the foreseeable future. However, the existence of the theory may alter that. The ability to travel to the stars and return within the lifetimes of those left behind will have a profound effect on mankind. It may even force the development of a unified world government and eliminate the need for a terrestrial military. What we find in the stars will determine whether a military of any kind will still be needed.

Psychic Technology

Although many people still consider psychic powers to be fantasy, several Governments have spent large sums to investigate their potential. Despite a few sensational books that have attempted to expose these programs, any real progress that may or may not have been made remains highly classified. Incontrovertible proof remains unavailable to anyone except those few willing to subject themselves to psychic training by the proponents of the field. Even personal experience with psychic powers can be questioned. However, given the obvious high degree of belief in one or more psychic phenomena by the general population, it is difficult to dismiss them entirely as frauds or delusions. If even a single segment of psychic technology proves to have a solid basis in reality, then it will have profound effects on how warfare and social intercourse are conducted.

There are many phenomena that are termed paranormal or psychic. However, if we keep an open mind as to their reality, there are at least five that have some serious military relevance: remote viewing, telepathy, remote influencing, telekinesis, and teleportation. Remote viewing is the area that has purported received the most governmental interest to date.[234],[235] A remote viewer enters a trance-like state in an environment free of significant external stimulation and is able to visualize remote locations. Such locations may be at great distances, inside of structures, and even located at other times (past and future). For example, one oft-repeated claim is that a remote viewer described the characteristics of the Typhoon submarine prior to its first satellite observation. The implications for intelligence and counter-intelligence would be substantial if remote viewing became fully accepted and could produce data that did not require substantiation by other means. However, in 1995 the Central Intelligence Agency commissioned the American Institutes for Research to perform an independent review of the Defense Intelligence Agency's "Star Gate" remote viewing program, which was being considered for transition to CIA control. It was concluded that although a statistically significant effect was clearly present, the source of this effect could not be identified with certainty as being paranormal in origin. Furthermore, there was no evidence that remote viewing was capable of providing operationally useful intelligence.[261] Using the results of this study as support, the CIA opted to officially remain out of the psychic intelligence field and the Star Gate program was terminated.

Telepathy is the ability to read other peoples minds. The intelligence and counter-intelligence implications are even greater than those of remote viewing. If the intent of military commanders or governmental leaders could be accurately determined, then any stratagem could be countered in advance.

Remote influencing is the ability not just to read other people's thoughts, but to influence those thoughts remotely. Think about the benefits that would derive from knowing the enemy plans in advance and having the enemy unconsciously sabotage the execution of his own plans.

Telekinesis is the ability to control the movement of objects at a distance. Think of the possibilities of causing the wrong switch to be closed at an inopportune moment on the control panel of a missile launch control system or a nuclear reactor. Mechanisms such as safe and arm devices might be impeded. Fuzes might be set off prematurely. Screws might be loosened causing subsequent failure of an aircraft access panel. Foreign objects might find their way into sensitive mechanisms.

Teleportation offers even more sinister opportunities. Consider the ability to cause a bomb to material inside an enemy headquarters when a staff meeting was underway. Mines could be made to materialize directly in the paths of ships or vehicles. Weapon systems could be moved about at random without the need for access paths. The possibilities are endless.

Space Colonies

Permanent space colonies, on the moon or the Lagrangian points in Earth orbit, have been technologically feasible for 30 years.[218] However, the cost of establishing such colonies has been beyond the means of any nation due to the high cost per pound of placing materials into Earth orbit. Not only must initial construction materials be lifted to the colony but also expendable materials such as food, water, and air must be periodically replaced. It is ultimately likely that these colonies could become entirely self-sufficient, although attempts to demonstrate the self-sufficiency of closed ecosystems have not yet been successful. Furthermore, new launch technologies may further reduce this economic constraint to growth. Experience obtained with the International Space Station (which just recently inaugurated permanent inhabitation) will probably go a long way towards furthering desires to establish permanent space colonies. All things considered, it is likely that permanent space colonies of some form will exist before the middle of the 21st Century and possibly within the next few decades.

If colonies are established by individual countries, primarily for the benefits of those countries, then should war between such countries break out on Earth, it may be difficult to continue to abide by the Outer Space Treaty and keep the colonies from becoming involved. On the other hand it is likely that all space colonies will have more in common with each other than with their parent countries. Coupled with the mutual dependence of each colony and its parent, this may foster closer international cooperation and ultimately force a true world government. If personnel interchange between the Earth and its space colonies occurs, then the discipline required for space colony life may ultimately modify the behavior of the earthbound in positive ways (for example, increased efforts at preservation of the environment).

NOTES AND REFERENCES

[1] CB 2010 Study Group, "Assessment of the Impact of Chemical and Biological Weapons on Joint Operations in 2010 (The CB 2010 Study: A Summary Report". Originally available on the Internet at http://www.nbc-med.org/publications/cb2010.htm. Many other documents have described all of these essential elements of power projection. This reference described them in a fashion that struck the author as particularly illuminating.

[2] Smith, Edward A., Blitzkrieg … From the Sea, draft Newport Paper, Naval War College, Chap. 6, "To See Ourselves as Others See Us", and Chap. 7, "Damn The Torpedoes" (May 1999).

[3] Mahnken, Tomas G., "Deny U.S. Access?" *U. S. Naval Institute Proceedings*, 124, 36-39 (September 1998).

[4] Office of the Chairman of the Joint Chiefs of Staff, *Joint Vision 2010*, (July 1996).

[5] Office of the Chairman of the Joint Chiefs of Staff, *Concept for Future Joint Operations: Expanding Joint Vision 2010*, (May 1997).

[6] Defense Science Board, "Investments in 21st Century Military Superiority", Summer Study (1995).

[7] Bowden, Mark, Black Hawk Down (Atlantic Monthly Press, New York NY, 1999).

[8] Kelly, John H., "Lebanon: 1982-1984", Chapter 6 in Jeremy R. Azrael & Emil A. Payin, U.S. and Russian Policymaking with Respect to the Use of Force, publication CF-129 (RAND Corporation, Santa Monica CA, 1996). Available on the Internet at http://www.rand.org/ publications/CF/CF129/CF-129.chapter6.html.

[9] On a visit to one of the Defense Department's Federal Contract Research Centers in early 1996, the author was shown some of the latest work on incorporating GPS guidance into Tomahawk. When he raised the issue of potential vulnerability to jamming, several different senior scientists assured the author that it was not possible to build a system capable of jamming the guidance system they had developed. Within a year an article appeared describing an inexpensive GPS jammer, see Reference 10. These individuals were apparently not familiar with the historical efficiency with which electronic combat specialists have degraded the performance of any electronic system of importance, see Reference 11. Nor were they apparently aware of Clarke's First Law, "When a distinguished but elderly scientist states that something is possible he is almost certainly right. When he states that something is impossible, he is very probably wrong." – Arthur C. Clarke, Profiles of the Future: An Inquiry into the Limits of the Possible.

[10] This claim has been attributed to Dr. Sean Gilmore of MIT Lincoln Laboratory in the following article by Herskovitz, Don, "And the Compass Spun Round and Round", *Journal*

of Electronic Defense, 20, #5, 35-39,65 (May 1997). Mr. Hugh V. Blanchard has made a similar claim (i.e., of being able to build a similar GPS jammer for as little as $400) on the Internet at *http://www.infowar.com/iwftp/c4i/archvol2/v02.n301.txt*.

[11] Price, Alfred, Instruments of Darkness: The History of Electronic Warfare (Charles Scribner's Sons, New York NY, 1977).

[12] Verne, Jules, Twenty Thousand Leagues under the Sea (Bantam Books, New York NY, 1962).

[13] Wells, Herbert George, The World Set Free (1914). Available on the Internet at *http://www.worldwideschool.org/library/books/lit/sciencefiction/TheWorldSetFree/toc.html*.

[14] Heinlein, Robert, Rocket Ship Galileo (Charles Scribner's Sons, New York NY, 1947).

[15] Clarke, Arthur C., 2001: A Space Odyssey (New American Library, New York NY, 1968).

[16] The author does not remember exactly where or when he heard or read this statement. The quotation is as accurate as he can remember. It is likely but not certain that the statement should be attributed to Arthur C. Clarke.

[17] Pike, John, "Nuclear Forces Guide", Federation of American Scientists (August 1999, updated regularly). This is a collection of multiple web pages that are available on the Internet at *http://www.fas.org/nuke/guide/index.html*.

[18] There are three critical components in a successful ICBM: the launch vehicle, an inertial guidance system, and a reentry vehicle. The launch vehicle needed to orbit a satellite (i.e., fire a "projectile" all the way around the world) is clearly more powerful than that needed to fire that same projectile half way around the world. However, some satellites are very small while reentry vehicles for operationally useful weapons are relatively large. Thus, the actual range achieved by a satellite launch vehicle converted to an ICBM will depend on how large a satellite it can launch. Nevertheless, any missile capable of placing into orbit payloads in excess of 500 kg can serve as a nuclear ICBM. Inertial guidance systems vary enormously in cost and complexity. Accuracy of warhead delivery is another factor the ICBM designer must face. See for example, Mackenzie, Ronald, Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance (MIT Press, Cambridge MA, 1993). If counterforce ICBM accuracy (accuracy high enough to place a nuclear warhead close enough to damage a hardened silo) is not necessary, and *it is not necessary if it is desired only to target large population centers*, then commercial aviation quality inertial guidance will suffice. Launching a satellite into a reasonable approximation of any desired orbit also requires an inertial guidance system of similar complexity. Combining readily available inertial navigation systems with global positioning system (GPS) navigation may provide still further improvements. Reentry vehicles do not need to be more complex than cones covered with ablative materials readily

available on the open market. However, unless carefully designed, the aerodynamics of reentry can cause large aimpoint errors. This may be catastrophic if pure fission weapons are delivered against relatively small targets, but unimportant if multi-megaton "city killer" hydrogen weapons are used against cities. Small motors causing the reentry vehicle to spin will improve the aerodynamics and improve accuracy. If low accuracy is required, the most difficult component is the launch vehicle. Consequently, any country capable of launching its own satellites could build ICBMs without much additional time or effort involved.

[19] Wade, Mark, "Encyclopedia Astronautica", (June 1999). This is a collection of web pages available on the Internet at *http://solar.rtd.utk.edu/~mwade/spaceflt.htm*.

[20] As this is being written the National Missile Defense program is once again undergoing significant changes. This precludes giving a complete and accurate description of the program. The current program changes will likely involve the proposed number of interceptors and their basing options. Fundamentally the program involves using kinetic energy kill vehicles carried by ground-based interceptor missiles. Targeting and initial guidance will be provided by a combination of ground-based radars and space-based infrared sensors. Hit-to-kill terminal guidance will be provided by an infrared seeker onboard each kill vehicle. For the latest officially released program description, interested persons should consult the Ballistic Missile Defense Office Internet site at *http://www.acq.osd.mil/bmdo/bmdolink/html/nmd.html*.

[21] The "Treaty between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems" was signed by the United States and the Soviet Union on 26 May 1972 and entered into force on 3 October 1972. A "Memorandum of Understanding on Succession" was mutually released on 26 September 1997. This memorandum stated that in agreement with the Lisbon Protocol to the Strategic Arms Reduction Treaty, the Ukraine, Belarus, Kazakhstan, and Russian Federation are bound by the Anti-Ballistic Missile treaty as successor states to the Union of Soviet Socialist Republics. A "Second Agreed Statement of 26 September 1997 Relating to the ABM Treaty" prohibited all testing of theater missile defense systems against targets with ranges in excess of 3500 km and velocities greater than 5.0 km/sec. Copies of the Treaty and other documents may be found on the Internet at *http://www.state.gov/www/global/arms/treaties/abm/abm2.html*.

[22] Feith, Douglas J. and Miron, George, "Memorandum of Law: Did the ABM Treaty of 1972 Remain in Force after the USSR Ceased to Exist in December 1991 and Did It Become a Treaty Between the United States and the Russian Federation?" Feith & Zell P.C. (24 February 1999). Available on the Internet at *http://www.actionworks.org/guides/missiles/abm.htm*.

[23] Rivkin, David B., Casey, Lee A., and Bartram, Darin R., "The Collapse of the Soviet Union and the End of the 1972 Anti-Ballistic Missile Treaty", Heritage Foundation (15 June 1998). Available on the Internet at *http://www.heritage.org/nationalsecurity/legalbrief/legal-brief.html*.

[24] "The Comprehensive Nuclear Test-Ban Treaty" was signed by the United States, Russian Federation, France, United Kingdom, China, and Israel on 24 September 1996. The treaty has not yet entered into force pending ratification by a sufficient number of signatories. North Korea, India, Pakistan, Iraq, and Cuba have not signed the treaty. Copies of the Treaty and other documents may be found on the Internet at *http://www.state.gov/www/global/arms/treaties/ctbt/ctbt.html*.

[25] Weisgall, Jonathan M., Operation Crossroads: The Atomic Tests at Bikini Atoll (Naval Institute Press, Annapolis MD, 1994).

[26] Pike, John, "States Possessing Weapons of Mass Destruction" Federation of American Scientists (16 October 1997). Available on the Internet at *http://www.fas.org/irp/threat/wmd_state.htm*.

[27] Chief of Naval Operations, Surface Ship Survivability Office, "U. S. Navy CBR Defense/U. S. Marine Corps NBC Defense Handbook", OPNAV P-86-1-95 (April 1995).

[28] Eldridge, John, "Maritime Aspects of NBC Defense", 6th CBW Protection Symposium, Stockholm, Sweden, 10-15 May 1998. Proceedings available on the Internet at *http://www.opcw.nl/cbwsymp/fullpapers/eldridge.htm*.

[29] Harney, Robert C., "Fighting Dirty? Sustaining Operations in A NBC Environment", Naval Postgraduate School Report NPS-IJWA-00-009 (7 November 1999).

[30] Crichton, Michael, The Andromeda Strain (Alfred A. Knopf, New York NY, 1979).

[31] Endicott, Stephen and Hagerman, Edward, The United States and Biological Warfare: Secrets from the Early Cold War and Korea (Indiana University Press, Bloomington IN, 1998), p. 73.

[32] United States Arms Control and Disarmament Agency, Arms Control Agreements and Disarmament Agreements: Texts and Histories of the Negotiations 1996 Ed. (U. S. Government Printing Office, Washington DC, 1996), p. 68.

[33] Richmond, Johnathan Y., and McKinney, Robert W. (Eds.), "Biosafety in Microbiological and Biomedical Laboratories", 3rd Ed., U. S. Department of Health and Human Services, HHS Publication No. (CDC) 93-8395 (U. S. Government Printing Office, Washington DC, May 1993).

[34] Hastings, Max, and Jenkins, Simon, The Battle for the Falklands (W. W. Norton, New York NY, 1983), pp. 151-156, 227-228, 296-297.

[35] Cordesman, Anthony H., and Wagner, Abraham R., The Lessons of Modern War, Vol. III, The Afghan and Falklands Conflict (Westview Press, Boulder CO, 1990), pp. 320-321.

[36] Cordesman, Anthony H., and Wagner, Abraham R., The Lessons of Modern War, Vol. II, The Iran-Iraq War (Westview Press, Boulder CO, 1990), pp. 282-290, 549-558.

[37] Johns Hopkins Applied Physics Lab, "The Cooperative Engagement Capability", Johns Hopkins APL Technical Digest, 16, #4, 377-396 (1995).

[38] The Net Assessment group in the Office of the Secretary of Defense regularly conducts wargames to determine the extent to which U. S. equipments, forces, force structures, and tactics are adequate to perform their directed missions in projected future threat environments. One intent of these games (among several others) is to identify probable adversary actions that could preclude successful mission accomplishment, so that the resulting deficiencies can be ameliorated by equipment development or force structure modifications. Red orders of battle are selected to be realistic projections with specific alterations made to enhance selected capabilities. That increased missile inventories have been included in these games is an indication of a high degree of concern about this adversary action being able to establish a potential vulnerability.

[39] Harney, Robert C., "Ducking the Punch or Absorbing the Blow? Letting the Anticipated Threat Drive Future Warship Design", Naval Postgraduate School Report NPS-IJWA-00-008 (7 November 1999).

[40] Gilreath, H. E., Driesman, A. S., Kroshl, W. M., White, M. E., Cartland, H. E., and Hunter, J. W., "Gun-Launched Satellites", *Johns Hopkins APL Technical Digest* 20, #3, 305-319 (July-September 1999).

[41] Murphy, C. H. and Bull, G. V., "Gun-Launched Sounding Rockets and Projectiles", *Ann. New York Acad. Sci.*, 140, 337 (1966).

[42] Lowther, William, Arms And the Man: Dr. Gerald Bull, Iraq, and the Supergun (Presidio Press, Novato CA, 1991).

[43] Anonymous, "Navy Theater Ballistic Missile Defense", a multicolor brochure published in September 1997 by the Program Executive Office (Theater Air Defense). This is a good unclassified overview of the Navy's TMD efforts.

[44] Pretty, Ronald T. (Ed.), "Pershing II" in Jane's Weapon Systems 1986-87 17th Ed. (Jane's Publishing, London UK, 1986), p.47.

[45] Parthasarathy, Anand, "In the service of the country", *Frontline*, 14, #25 (13-26 December 1997). Available on the Internet at *http://www.the-hindu.com/fline/fl1425/14251070.htm*.

[46] Anonymous, "Agni IRBM", *Bharat Rakshak.* Available on the Internet at *http://www.bharat-rakshak.com/MISSILES/Agni.html*.

[47] Fisher, Jr., Richard D., "China Increases Its Missile Forces While Opposing U. S. Missile Defense", The Heritage Foundation, Backgrounder No. 1268 (7 April 1999). Available on the Internet at *http://www.heritage.org/library/backgrounder/bg1268.html*.

[48] Anonymous, "The Chinese Missile Threat", Center for Defence and International Security Studies, Lancaster University, UK (1997). Available on the Internet at *http://www.cdiss.org/China_Essay.htm*.

[49] Many papers and concepts for transatmospheric aircraft are contained in the U. S. Air Force study of the future entitled Air Force 2025, (August 1996). Available on the Internet at *http://www.au.af.mil/au/2025/*.

[50] Anonymous, "RLV Alert", *SpaceDaily* (17 September 1999). Available on the Internet at *http://www.spacedaily.com/rlv.html*.

[51] The "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies" was signed on 27 January 1967 and entered into force on 10 October 1967. The treaty explicitly prohibits orbiting nuclear weapons or carrying nuclear weapons into space. All probable nuclear weapon states with the exception of North Korea have signed or acceded to this treaty, although Iran never ratified the treaty after signing. Copies of the Treaty and other documents may be found on the Internet at *http://www.state.gov/www/global/arms/treaties/space1.html*.

[52] Hartmann, Gregory K. and Truver, Scott C., Weapons That Wait (Naval Institute Press, Annapolis MD, 1991).

[53] Kaminski, Paul D., "Three Musts for Affordable Naval Mine Warfare", *Defense Issues*, 11, #69 (11 June 1996). Available on the Internet at *http://www.defenselink.mil/speeches/1996/ 219960611-kaminski.html*.

[54] Agresti III, Michael C., "Mr. Connie Agresti: Spring, 1997", correspondence (1997). Available on the Internet at *http://www.west.ga.net/~stquesin/agrest97.htm*.

[55] Jordan, Stephanie L., "Navy dedicates resources to sea-mine hunting", *Corpus Christi Caller-Times* (4 October 1998). Available on the Internet at *http://wwwkw.caller.com/news98/ news21278.html*.

[56] Naval Historical Center, "U. S. Navy in Desert Shield/Desert Storm", Department of the Navy (15 May 1991). Available on the Internet at *http://www.history.navy.mil/wars/ dstorm/index.html*.

[57] Watson, Bruce W., George, B., Tsouras, P., and Cyr, B. L., Military Lessons of the Gulf War (Presidio Press, Novato CA, 1991), pp. 125-127.

[58] Cordesman, Anthony H., and Wagner, Abraham R., The Lessons of Modern War, Vol. IV, The Gulf War (Westview Press, Boulder CO, 1996), pp. 810-818, 820-825.

[59] Baker III, A. D., The Naval Institute Guide to Combat Fleets of the World 1998-1999 (Naval Institute Press, Annapolis MD, 1998).

[60] Thun, Rose, "Surface Ship Torpedo Defense Case Study", Navy Acquisition Center of Excellence, Washington DC (28 July 1998). This viewgraph presentation gives limited details on the SSTD program. Available on the Internet at *http://www.ace.navy.mil/public/events/bmp/ ACECASE/index.htm*.

[61] Burcher, Roy and Rydill, Louis, Concepts in Submarine Design (Cambridge University Press, Cambridge UK, 1994), Chap. 6.

[62] Burton, Russell R. and Whinnery, James E., "Biodynamics: Sustained Acceleration", Chapter 9 in DeHart, Roy L. (Ed.), Fundamentals of Aerospace Medicine 2nd Ed. (Williams & Wilkins, Baltimore MD, 1996). The average unprotected adult experiences tunnel vision at a mean acceleration load of 4.1 +/- 0.7g, complete loss of vision (blackout) at 4.8 +/- 0.8g, and unconsciousness at 5.4 +/- 0.9g. With the protection of a g-suit, these levels increase by about 1.0-1.5g. Physically-trained, combat pilots in g-suits and using anti-g straining maneuvers and positive pressure breathing can increase their g-tolerance up to a level of 9.0g or slightly higher. Although a few rare individuals may have a tolerance near or slightly above 10g, for the most part we do not know how to keep the average combat pilot from suffering g-induced loss of consciousness (G-LOC) at accelerations above 10g.

[63] Intel Corporation, "What is Moore's Law", Intel Museum (1999). Available on the Internet at *http://www.intel.com/intel/museum/25anniv/hof/moore.htm*.

[64] Jenn, David C., Radar and Laser Cross Section Engineering (American Institute of Aeronautics and Astronautics, Washington DC, 1995).

[65] Jones, J., Stealth Technology: The Art of Black Magic (TAB Books, Blue Ridge Summit PA, 1989).

[66] Richardson, Doug, Stealth: Deception, Evasion, and Concealment in the Air (Crown Publishers, New York NY, 1989).

[67] U. S. Government Accounting Office, "B-2 Bomber: Cost and Operational Issues", GAO/NSIAD-97-181 (August 1997).

[68] Farrell, Jay A. and Barth, Matthew, The Global Positioning System & Inertial Navigation (McGraw-Hill, New York NY, 1999), Chap. 5.

[69] Lee, R. G., Garland-Collins, T. K., Johnson, D. E., Archer, E., Sparkes, C., Moss, G. M., & Mowat, A. W., Guided Weapons (Brassey's Defence Publishers, London UK, 1988).

[70] James, D. A., Radar Homing Guidance for Tactical Missiles (Macmillan, London UK, 1986).

[71] McDaid, Hugh and Oliver, David, Smart Weapons (Orion Publishing, New York NY, 1997).

[72] Couhat, Jean L., Combat Fleets of the World, 1982/83 (Naval Institute Press, Annapolis MD, 1982) pp. 234, 238.

[73] Brown, David, The Royal Navy and the Falklands War (Arrow Books, London UK, 1987), p. 228.

[74] Ghose, Rabindra N., EMP Environment and System Hardness Design (Don White Consultants, Gainesville VA, 1983).

[75] Saxton, Jim, O'Bryon, James, Schriner, David, Merritt, Ira, and Kehs, Alan, Joint Economic Committee Hearing on "Radio Frequency Weapons and Proliferation: Potential Impact on the Economy", (25 February 1998). Available on the Internet at *http://www.house.gov/jec/ hearings/02-25-8h.htm*.

[76] Benford, James, and Swegle, John, High-Power Microwaves (Artech House, Norwood MA, 1992).

[77] Maiman, Theodore H., "Stimulated Optical Radiation in Ruby", *Nature,* 187, 493-493 (6 August 1960). This is the first published account of laser action.

[78] Anonymous, "'Light Ray' – Fantastic Weapon of the Future?", *U. S. News and World Report* LII, #14, 47-50 (2 April 1962). This is the first popular press description of lasers as missile killers of which the author is aware. Note that it was published a mere 20 months after Maiman's demonstration of the first working laser. None of the lasers currently being considered for missile defense had been invented at the time of publication of this article.

[79] Duffner, Robert W., Airborne Laser: Bullets of Light (Plenum Press, New York NY, 1997).

[80] Hecht, Jeff, Beam Weapons (Plenum Press, New York NY, 1984).

[81] Bloembergen, N., Patel, C. K. N., et al, "Report to the American Physical Society of the study group on science and technology of directed energy weapons", *Rev. Mod. Phys.,* 59, Part II, #3, S1-S200 (July 1987).

[82] Anonymous, "HELSTF: U. S. Army High Energy Laser Systems Test Facility", brochure published by U. S. Army Space and Strategic Defense Command, Public Affairs Office, P. O. Box 15280, Arlington, VA 22215-0280. HELSTF is the site at White Sands

Missile Range where the MIRACL chemical laser and SEALITE Beam Director are located.

[83] Tyson, Robert K., Principles of Adaptive Optics (Academic Press, London UK, 1991).

[84] U. S. Army Space and Missile Defense Command, "Tactical High Energy Laser: Twenty-First Century Air Defense", Fact Sheet (undated). Available on the Internet at *http://www.smdc.army.mil/FactSheets/THEL.html*.

[85] Anonymous, "ABL YAL 1A", Fact Sheet on the USAF Airborne Laser (undated). Available on the Internet at *http://www.airforce-technology.com/projects/abl/index.html*.

[86] Pike, John, "Space-Based Laser", Federation of American Scientists (9 February 1999). Available on the Internet at *http://www.fas.org/spp/starwars/program/sbl.htm*.

[87] Brau, Charles A., Free-Electron Lasers (Academic Press, San Diego CA, 1990).

[88] Cebrowski, Arthur K. and Garstka, John J., "Network-Centric Warfare: Its Origin and Future", *U.S. Naval Institute Proceedings*, 124, #1, 28-35 (January 1998).

[89] Schwartau, Winn, Information Warfare 2nd Ed. (Thunder's Mouth Press, New York NY, 1996).

[90] Libicki, Martin C., What is Information Warfare? (National Defense University Press, Washington DC, 1996).

[91] Arquilla, John and Ronfeldt, David, In Athena's Camp: Preparing for Conflict in the Information Age (RAND, Santa Monica CA, 1997).

[92] Frank, Douglas, "The Internet Worm" on the E-Mail Privacy Page (1997). Available on the Internet at *http://rhet.agri.umn.edu/Rhetoric/misc/dfrank/worminfo.html*.

[93] Kehoe, Brendan P., "The Internet Worm" in Zen and the Art of the Internet (January 1992). This apparently unpublished handbook is available on the Internet at *http://www.cs.indiana.edu/docproject/zen/zen-1.0_toc.html* .

[94] Clancy, Tom, The Bear and the Dragon (G. P. Putnam's Sons, New York NY, 2000), p.206.

[95] Anderberg, Bengt and Wolbarsht, Myron L., Laser Weapons: The Dawn of a New Military Age (Plenum Press, New York NY, 1992).

[96] Morchin, William C., Airborne Early Warning Radar (Artech House, Norwood MA, 1990), Chap. 1.

[97] Chaisson, Kernan, "Airborne Surveillance Takes Command", *Journal of Electronic Defense*, (January 1999).

[98] Dewar, Michael, The Art of Deception in Warfare (David & Charles Publishers, Newton Abbot UK, 1989).

[99] Brown, Anthony Cave, Bodyguard of Lies (Harper and Row, New York NY, 1975).

[100] McDonald, Robert A., "CORONA: Success for Space Reconnaissance, A Look into the Cold War, and a Revolution for Intelligence", *Photogrammetric Engineering & Remote Sensing*, LXI, #6, 689-720 (June 1995).

[101] Toliver, Raymond F. and Constable, Trevor J., Fighter General: The Life of Adolf Galland (AmPress Publishing, Zephyr Cove NV, 1990), Chaps. 1 & 2.

[102] Groom Lake is the geographic identification of a restricted access facility located on the Nellis AFB Test Range near the northeast corner of the Department of Energy's Nevada Test Site. Presumably it is a flight test facility given the impressive runway facilities obvious in commercial satellite imagery of the site. Tests are presumably conducted only at night and when there are no known intelligence satellite overflights. All equipment is likely kept out of sight in large hangars when actual tests are not in progress. Stringent physical security measures keep unauthorized visitors from gaining access to the site. Satellite photography and "outsider" humint therefore reveal no information other than the existence of a substantial base with a long airstrip that has no obvious users. Given the available "intelligence", Groom Lake could be almost anything from a flight test center for classified aircraft to a "home base for flying saucers" to a "retirement" facility for "unreliable" former intelligence officers to an elaborate decoy designed to draw attention away from sites where truly "interesting" activities are being pursued.

[103] Waller, Douglas C., The Commandos (Simon & Schuster, New York NY, 1994), Chap. 5.

[104] Marcinko, Richard and Weisman, John, Rogue Warrior (Simon & Schuster, New York NY 1992).

[105] Dupuy, R. Ernest and Dupuy, Trevor N., The Harper Encyclopedia of Military History 4th Ed. (Harper Collins, New York NY, 1993) p.1108.

[106] Orita, Zenji and Harrington, Joseph D., I-Boat Captain (Major Books, Canoga Park CA, 1976) pp. 47-50.

[107] Williams, Peter and Wallace, David, Unit 731: Japan's Secret Biological Warfare in World War II (Free Press, New York NY, 1989) pp. 124-127.

[108] Ambrose, Stephen E., D-Day, June 6, 1944: The Climactic Battle of World War II (Simon & Schuster, New York NY, 1994), Chap. 10.

[109] Parker, Danny S., Battle of the Bulge: Hitler's Ardennes Offensive, 1944-1945 (Combined Books, Conshohocken PA, 1991), pp. 188-194.

[110] Bowditch, Nathaniel, American Practical Navigator: An Epitome of Navigation, Vol. 1 Defense Mapping Agency Hydrographic/Topographic Center Publication No. 9 (U. S. Government Printing Office, Washington DC, 1984), p.1312.

[111] Seagraves, Mary Ann and Szymber, Richard J., "Weather: A Force Multiplier", *Military Review*, LXXV, #6, 69-76 (November-December 1995).

[112] House, Tamzy J., Near, Jr., James B., Shields, William B., Celentano, Ronald J., Husband, David M., Mercer, Ann E. and Pugh, James E., "Weather as a Force Multiplier: Owning the Weather in 2025" in Air Force 2025 (August 1996). Available on the Internet at *http://www.au.af.mil/au/2025/volume3/chap15/v3c15-1.html*.

[113] Fishman, Jack, and Kalish, Robert, The Weather Revolution: Innovations and Imminent Breakthroughs in Accurate Forecasting (Plenum Press, New York NY, 1994).

[114] Measures, Raymond M., Laser Remote Sensing (Krieger Publishing, Malabar FL, 1992).

[115] Matthews, Robert, "The Weather Man", *New Scientist*, 167, #2251, 24-29 (12 August 2000).

[116] Typical hurricanes (or typhoons or tropical cyclones) have peak wind speeds ranging from 33 m/s to speeds well over 70 m/s. They may have effective diameters ranging from about 300 km to over 1500 km. The energy contained in a hurricane is in two forms: kinetic energy of the wind and potential energy in warm water vapor. Condensation of the water vapor releases the energy that drives the winds. The kinetic energy component can be estimated from the relation $KE = 0.5\ \rho_a\ h\ (\pi r^2)\ v^2$ where ρ_a is the density of the atmosphere (approximately 1.2 kg/m^3 at sea level), h is the scale height of the atmosphere (approx. 10 km), r is the radius of the hurricane, and v is the peak wind velocity (at the surface – winds actually increase significantly as altitude increases). For a nominal hurricane with 300-km radius and 50 m/s winds, we calculate 4.2×10^{18} J. For the ranges of size and velocity of observed hurricanes we get the 10^{18}-10^{20} J energy range. The power of a hurricane can be estimated by dividing its kinetic energy by the time it takes for that energy to dissipate. This can be obtained from the lifetime of the hurricane after it moves onto land. On land, evaporation from warm ocean water (the source of the energy) is no longer present. Typical lifetimes over land range from a few hours (10^4 s) to a day (10^5 s). Thus, typical hurricane powers are estimated to lie in the range 10^{13}-10^{16} W.

[117] The "Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques" was signed by the United States, United Kingdom, Union of Soviet Socialist Republics, and many other states on 18 May 1977 and entered into force on 5 October 1978. Among other things it prohibits altering the weather to further

military or other hostile ends. A copy of the Convention may be found on the Internet at *http://www.state.gov/global/arms/treaties/environ1.html*.

[118] Multiple Military Departments, "NLW – Multiservice Procedure for the Tactical Employment of Nonlethal Weapons", FM 90-40, MCRP 3-15.8, NWP 3-07.31, & USCG PUB 3-07.31 (October 1998).

[119] Air Mobility Command, "Civil Reserve Air Fleet", United States Air Force Fact Sheet (May 1999). Available on the Internet at *http://www.af.mil/news/factsheets/Civil_Reserve_Air_Fleet.html* .

[120] Pike, John, "Sealift", Federation of Atomic Scientists (7 December 1998). Available on the Internet at *http://www.fas.org/man/dod-101/sys/ship/sealift.htm*.

[121] Richards, Kim A., "Prepo Afloat: Key to Power Projection", *Army Logistician* (January 1998). Available on the Internet at *http://www.fas.org/man/dod-101/sys/ship/docs/alog-980100-ms258.htm*.

[122] Regan, Geoffrey, Blue on Blue: A History of Friendly Fire (Avon Books, New York NY, 1995).

[123] U. S. Congress, Office of Technology Assessment, Who Goes There: Friend or Foe?, OTA-ISC-537 (U. S. Government Printing Office, Washington DC, June 1993).

[124] Glines, Carroll V., The Doolittle Raid (Orion Books, New York NY, 1988).

[125] Staff of U. S. News & World Report, Triumph Without Victory (Random House, New York NY, 1992), pp. 270-271.

[126] Atkinson, Rick, Crusade: The Untold Story of the Persian Gulf War (Houghton Mifflin, Boston MA, 1993), pp. 189-213.

[127] Reisman, W. Michael and Antoniou, Chris T., The Laws of War: A Comprehensive Collection of Primary Documents on International Laws Governing Armed Conflicts (Random House, New York NY, 1994).

[128] McKee, Alexander, Dresden 1945: The Devil's Tinderbox (E. P. Dutton, New York NY, 1982). The Hamburg firestorm resulting from multiple raids in July 1943 produced 48,000 casualties, p. 59; The Dresden firestorm resulting from raids on the nights of 13-14 and 15 February 1945 produced more than 35,000 casualties and possibly as high as 250,000 casualties, pp. 321-322. Most of the casualties were civilians.

[129] Rogers, Will and Rogers, Sharon, with Gregston, Gene, Storm Center: The *USS Vincennes* and Iran Air Flight 655 (Naval Institute Press, Annapolis MD, 1992).

[130] Hickam, Jr., Homer H., Rocket Boys (Delacorte Press, New York NY, 1998). This autobiography formed the basis for the movie, October Sky, directed by Joe Johnston and released by Universal Studios in 1999.

[131] Christensen, Clayton, "Disruptive Technologies" (1999). Available on the Internet at *http://www.disruptivetechnologies.com/*.

[132] Glasstone, Samuel and Dolan, Philip J., The Effects of Nuclear Weapons 3rd Ed. (U. S. Government Printing Office, Washington DC, 1977).

[133] Hansen, Chuck, U. S. Nuclear Weapons: The Secret History, (Orion books, New York NY, 1988).

[134] Sublette, Carey, Nuclear Weapons Frequently Asked Questions version 2.21 (7 January 1998). Available on the Internet at *http://www.fas.org/nuke/hew/Nwfaq/Nfaq0.html*.

[135] United States Army - Office of the Surgeon General, Handbook on the Medical Aspects of NBC Defensive Operations, Field Manual FM 8-9 (1 February 1996). Available on the Internet at *http://www.nbc-med.org/amedp6/index.htm*.

[136] U. S. Congress, Office of Technology Assessment, Technologies Underlying Weapons of Mass Destruction, OTA-BP-ISC-115 (U. S. Government Printing Office, Washington DC, December 1993).

[137] Stockholm International Peace Research Institute (SIPRI), The Problem of Chemical and Biological Warfare. Volume II. CB Weapons Today (Almqvist & Wiksell, Stockholm, Sweden, 1973).

[138] U. S. Army Medical Research Institute of Infectious Diseases, Medical Management of Biological Casualties Handbook, 3rd Ed. (July 1998), available on Internet at *http://www.nbc-med.org/SiteContent/OnlineRef/FieldManuals/medman/Cover.htm*.

[139] Alibek, Ken and Handelman, Stephen, Biohazard (Random House, New York NY, 1999).

[140] Wilson, M. E., A World Guide to Infections (Oxford University Press, Oxford UK, 1991).

[141] Benenson, Abram S. (Ed.), Control of Communicable Diseases Manual, 16th Ed. (American Public Health Association, Washington DC, 1995).

[142] Departments of the Army and Air Force, "Military Biology and Biological Warfare Agents", Technical Manual TM 3-216/ AFM 355-6 (11 January 1956). Reprinted as Guide to Germ Warfare (Desert Publications, El Dorado AR, 1978).

[143] Edgewood Research, Development, & Engineering Center, "Military Unique Material Safety Data Sheets from the Edgewood Safety Office", United States Army (various dates). Available on the Internet at *http://www.cbdcom.apgea.army.mil/RDA/erdec/risk/safety/msds/*.

[144] U. S. Army Medical Research Institute of Chemical Defense, Medical Management of Chemical Casualties Handbook, 2nd Ed. (September 1995), available on Internet at *http://chemdef.apgea.army.mil/chemcasu/titlepg.htm*.

[145] Department of the Army, "Military Chemistry and Chemical Agents", Technical Manual TM 3-215 (August 1956).

[146] Prentiss, Augustin M., Chemicals in War (McGraw-Hill Book Co., New York NY, 1937).

[147] Somani, Satu M., Chemical Warfare Agents (Academic Press, San Diego CA, 1992).

[148] Marrs, Timothy C., Maynard, Robert L., and Sidell, Frederick R., Chemical Warfare Agents: Toxicology and Treatment (John Wiley & Sons, New York NY, 1996).

[149] Walker, F. William, Parrington, Josef R., and Feiner, Frank, Nuclides and Isotopes14th Ed. (General Electric Company Nuclear Energy Operations, San Jose CA, 1989).

[150] Lederer, C. Michael and Shirley, Virginia S. (Eds.), Table of Isotopes 7th Ed. (John Wiley & Sons, New York NY, 1978).

[151] Conklin, James J. and Walker, Richard I., Military Radiobiology (Academic Press, Orlando FL, 1987).

[152] Shapiro, Jacob, Radiation Protection: A Guide for Scientists and Physicians 3rd Ed. (Harvard University Press, Cambridge MA, 1990).

[153] U. S. Congress, Office of Technology Assessment, Proliferation of Weapons of Mass Destruction: Assessing the Risks, OTA-ISC-559 (U. S. Government Printing Office, Washington DC, August 1993).

[154] The "Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Elimination of Their Intermediate-Range and Shorter-Range Missiles"). This treaty was signed by the U. S. and the U. S. S. R. on 8 December 1987 and entered force on 1 June 1988. Copies of the treaty and other documents may be found on the Internet at *http://www.state.gov/www/global/arms/treaties/inf1.html*.

[155] National Air Intelligence Center, "Ballistic and Cruise Missile Threat" (1998). Available on the Internet at *http://www.fas.org/irp/threat/missile/naic/index.html*.

[156] Nathanson, Fred E., Radar Design Principles 2nd Ed. (McGraw-Hill Book Co., New York NY, 1991) p. 275 sea clutter. Ship cross section.

[157] Skolnik, Merrill I., Introduction to Radar Systems 2nd Ed. (McGraw-Hill Book Co., New York NY, 1980).

[158] Knott, Eugene F., Shaeffer, John F., and Tuley, Michael T., Radar Cross Section (Artech House, Norwood MA, 1985).

[159] Schleher, D. Curtis, Introduction to Electronic Warfare (Artech House, Norwood MA, 1986).

[160] Broad, William J., Teller's War (Simon & Schuster, New York NY, 1992).

[161] Verdeyen, Joseph T., Laser Electronics 2nd Ed. (Prentice-Hall, Englewood Cliffs NJ, 1989).

[162] Anderson, J. D., Gasdynamic Lasers (Academic Press, San Diego CA, 1976).

[163] Gross, Rolf W. F. and Bott, Jerry F., Handbook of Chemical Lasers (John Wiley & Sons, New York NY, 1976).

[164] Geary, Joseph M., Introduction to Wavefront Sensors (SPIE Press, Bellingham WA, 1995).

[165] Sliney, D. and Wolbarsht, M., Safety with Lasers and Other Optical Sources: A Comprehensive Handbook (Plenum Press, New York NY, 1980), Ch. 4.

[166] Dupuy, R. Ernest, and Dupuy, Trevor N. (Eds.), The Harper Encyclopedia of Military History 4th Ed. (Harper Collins Publishers, New York NY, 1993), pp. 939-942.

[167] Mish, Frederick C. (Editor in Chief), Merriam Webster's Collegiate Dictionary 10th Ed. (Merriam-Webster, Springfield MA, 1993). This was used as the source for most "diplomatic" definitions although occasionally the author has modified or elaborated a definition where he felt it was necessary.

[168] United States Arms Control and Disarmament Agency, Arms Control and Disarmament Agreements: Texts and Histories of the Negotiations 1996 Ed. (U. S. Government Printing Office, Washington DC, 1996).

[169] Faculty of Law, "Centenary of the 1899 Hague Peace Conference", University of Melbourne, Australia (undated). This document is available on the Internet at *http://www.law.unimelb.edu.au/even...ference/1899_hague_conference.html*.

[170] "Convention with Respect to the Laws and Customs of War on Land" (29 July 1899). Text available on the Internet at *http://www.lib.byu.edu/~rdh/wwi/hague/hague2.html.*

[171] "Convention Respecting the Laws and Customs of War on Land" (18 October 1907). Text available on the Internet at *http://www.lib.byu.edu/~rdh/wwi/hague/hague5.html.*

[172] Richter, Donald, Chemical Soldiers: British Gas Warfare in World War I (University of Kansas Press, Lawrence KS, 1992), p.16.

[173] "Protocol for the Prohibition of Poisonous Gases and Bacteriological Methods of Warfare" (17 June 1925). Text available on the Internet at *http://www.state.gov/www/global/arms/treaties/geneva1.htm* or *http://projects.sipri.se/cbw/docs/cbw-hist-geneva-eng.html*.

[174] "Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction" (8 August 1994). Available on the Internet at *http://www.state.gov/www/global/arms/treaties/cwctext.htm* or *http://www.sipri.se/projects/group-cw/Part1.html* through */Part6.html.*

[175] "Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction" (10 April 1972). Text available on the Internet at *http://www.state.gov/www/global/arms/treaties/bwc1.htm* or *http://www.sipri.se/cbw/docs/bw-bwtc-text.html*.

[176] United States Congress, "The Antiterrorism and Effective Death Penalty Act of 1996", Public Law 104-132 (24 April 1996).

[177] Centers for Disease Control and Prevention, "Additional Requirements for Facilities Transferring or Receiving Select Agents; Final Rule", 42 CFR Part 72, *Federal Register*, 61, #207, 55189-55200 (24 October 1996).

[178] Working Group on Biological and Toxin Weapons Verification, "Beyond VEREX: A Legally Binding Compliance Regime for the Biological and Toxin Weapons Convention", Federation of Atomic Scientists (July 1994). Available on the Internet at *http://www.fas.org/bwc/verex.html*.

[179] "Treaty on the Non-Proliferation of Nuclear Weapons" (1 July 1968). Text available on the Internet at *http://www.state.gov/www/global/arms/treaties/npt1.html* or *http://www.iaea.or.at/worldatom/glance/legal/npttext.html*.

[180] "Protocol to the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms" (23 May 1992). Text available on the Internet at *http://www.state.gov/www/global/arms/starthtm/start/lisbon.html*.

[181] "1995 Review and Extension Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons. Final Document. Part I. Organization and work of the Conference" (1995). Text Available on the Internet at *http://www.fas.org/nuke/control/npt/docs/2142.htm*.

[182] IAEA, "The Structure and Content of Agreements Between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons", IAEA Information Circular INFCIRC/153 (Corrected) (June 1972). Text available on the Internet at *http://www.iaea.or.at/worldatom/infcircs/inf153.html*.

[183] "Agreement Between the United States of America and the International Atomic Energy Agency for the Application of Safeguards in the United States (and Protocol Thereto)" (18 November 1977). Text available on the Internet at *http://www.state.gov/www/global/arms/treaties/usiaea1.html* through *~/usiaea3.html*.

[184] IAEA, "The Agency's Safeguards System 1965, as Provisionally Extended in 1966 and 1968", IAEA Information Circular INFCIRC/66/Rev.2 (16 September 1968). Text available on the Internet at *http://www.iaea.or.at/worldatom/infcircs/inf66r2/html*.

[185] Leventhal, Paul, "Safeguards Shortcomings – A Critique", Nuclear Control Institute (12 September 1994). Available on the Internet at *http://www.nci.org/plsgrds.htm*.

[186] "Model Protocol Additional to the Agreement(s) Between State(s) and the International Atomic Energy Agency for the Application of Safeguards", IAEA Information Circular INFCIRC/540(Corrected)(September 1997). Text available on the Internet at *http://wwww.iaea.or.at/worldatom/infcircs/infcirc540corrected.pdf*.

[187] "Convention on the Physical Protection of Nuclear Material" (3 March 1980). Text available on the Internet at *http://www.state.gov/www/global/arms/treaties/nucmate1.html*.

[188] Harney, Robert C., Unconventional Weapons of Mass Destruction (WMD) and Terrorism (Naval Postgraduate School, Monterey CA, 2000).

[189] "Treaty Banning Nuclear Weapons Tests in the Atmosphere, in Outer Space and Under Water" (5 August 1963). Text available on the Internet at *http://www.state.gov/www/global/arms/treaties/ltbt1.html*.

[190] "Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Underground Nuclear Weapon Tests (and Protocol Thereto)" (3 July 1974). Text available on the Internet at *http://www.state.gov/www/global/arms/treaties/ttbt1.html*.

[191] "Treaty Between the United States of America and the Union of Soviet Socialist Republics on Underground Nuclear Explosions for Peaceful Purposes (and Protocol Thereto)" (28 May 1976). Text available on the Internet at

http://www.state.gov/www/global/arms/treaties/pne1.html.

[192] "Treaty for the Prohibition of Nuclear Weapons in Latin America" (14 February 1967). Text available on the Internet at http://www.state.gov/www/global/arms/treaties/latin1.html.

[193] "South Pacific Nuclear Free Zone Treaty" (8 August 1986). Text available on the Internet at http://www.state.gov/www/global/arms/treaties/spnfz.html.

[194] "The African Nuclear-Weapon-Free Zone Treaty (The Treaty of Pelindaba)" (11 April 1996). Text available on the Internet at http://www.state.gov/www/global/arms/treaties/afrinwfz.html.

[195] "Treaty on the Southeast Asia Nuclear Weapon-Free Zone" (15 December 1995). Text available on the Internet at http://www.aseansec.org/politics/pol_agr7.htm.

[196] Pande, Savita, "Prospects of Nuclear Weapon-Free Zones: South-East Asia and Central Asia" ( ). Available on the Internet at http://www.idsa-india.org/an-sep8-4.html.

[197] "The Antarctic Treaty" (1 December 1959). Text available on the Internet at http://www.state.gov/www/global/arms/treaties/arctic1.html.

[198] "Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Seabed and the Ocean Floor and in the Subsoil Thereof" (11 February 1971). Text available on the Internet at http://www.state.gov/www/global/arms/treaties/seabed1.html.

[199] Bureau of Nonproliferation, "The Missile Technology Control Regime", U. S. Department of State (15 September 1997). Text available on the Internet at http://www.state.gov/www/global/arms/np/mtcr/mtcr96.html.

[200] "Missile Technology Control Regime" (7 January 1993). Text available on the Internet at http://www.state.gov/www/global/arms/np/mtcr/mtcr_anx.html.

[201] "Agreed Statements, Common Understandings, and Unilateral Statements Regarding the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems" (26 May 1972). Text available on the Internet at http://www.state.gov/www/global/arms/treaties/abm/abm3.html.

[202] "Protocol to the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems" (3 July 1974). Text available on the Internet at http://www.state.gov/www/global/arms/treaties/abm/abmprot1.html.

[203] "Memorandum of Understanding Relating to the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems of 26 May 1972" (26 September 1997). Text available on the Internet at *http://www.state.gov/www/global/arms/factsheets/missdef/abm_mou.html*.

[204] "Standing Consultative Commission Second Agreed Statement Relating to the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Anti-Ballistic Missile Systems of 26 May 1972" (26 September 1997). Text available on the Internet at *http://www.state.gov/www/global/arms/factsheets/missdef/abm_scc2.html*.

[205] "Strategic Arms Limitation Talks (SALT I)" (undated). Text available on the Internet at *http://www.state.gov/www/global/arms/treaties/salt1.html*.

[206] "Interim Agreement Between the United States of America and the Union of Soviet Socialist Republics on Certain Measures With Respect to the Limitation of Strategic Offensive Arms" (26 May 1972). Text available on the Internet at *http://www.state.gov/www/global/arms/treaties/interim1.html*.

[207] "Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Limitation of Strategic Offensive Arms" (18 June 1979). Text available on the Internet at *http://www.state.gov/www/global/arms/treaties/salt2-1.html* through *~/salt2-4.html*.

[208] "Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms" (31 July 1991). Text available on the Internet at *http://www.state.gov/www/global/arms/starthtm/start/treatytc.html*.

[209] "Protocol on Procedures Governing the Conversion or Elimination of the Items Subject to the Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms" (31 July 1991). Text available on the Internet at *http://www.state.gov/www/global/arms/starthtm/start/convpro.html*.

[210] "Treaty Between the United States of America and the Union of Soviet Socialist Republics on Further Reduction and Limitation of Strategic Offensive Arms" (3 January 1993). Text available on the Internet at *http://www.state.gov/www/global/arms/starthtm/start2/st2intal.html* .

[211] "Fissile Material Production Cutoff Treaty (FMCT) Negotiations", Arms Control and Disarmament Agency (27 March 1997). Text available on the Internet at *http://www.acda.gov/factshee/wmd/nuclear/fissile/fissneg.htm.*

[212] "Treaty on Open Skies" (24 March 1992). Text available on the Internet at *http://www.state.gov/www/global/arms/treaties/openski1.html*.

[213] Harney, Robert C., “Technology Assessment for Strategic Planning and Military Innovation”, Naval Postgraduate School Report (to be published).

[214] Price, Derek J. de Solla, Little Science, Big Science (Columbia University Press, New York NY, 1963).

[215] Banks, Danny, “Introduction to Microengineering” (26 April 1999). Available on the Internet at *http://dbanks.demon.co.uk/ueng/*.

[216] Tuck, Clive D. S.(Ed.), Modern Battery Technology (Simon & Schuster, New York NY, 1991).

[217] Yu, Min-Feng, Files, Bradley S., Arepalli, Sivaram, and Ruoff, Rodney S., “Tensile Loading of Ropes of Single Wall Carbon Nanotubes and their Mechanical Properties”, *Phys. Rev. Letts.,* 84, 5552 (12 June 2000).

[218] Johnson, Richard D. and Holbrow, Charles (Eds.), Space Settlements: A Design Study, NASA Publication SP-413 (U. S. Government Printing Office, Washington DC, 1977).

[219] Arthur C. Clarke, The Fountains of Paradise (Harcourt Brace, New York NY, 1978).

[220] Kittel, Charles, Introduction to Solid State Physics 4^{th} Ed. (John Wiley & Sons, New York NY, 1971), Chap. 12.

[221] Beaudette, Charles G., Excess Heat: Why Cold Fusion Research Prevailed (Oak Grove Press, South Bristol ME, 2000).

[222] Bardeen, J., Cooper, L.N., and Schrieffer, J. R., *Phys. Rev.*, 106, 162 (1957) and *Phys. Rev.*, 108, 1175 (1957).

[223] Milburn, Gerard J., The Feynman Processor (Perseus Books, Reading MA, 1998).

[224] Hamilton, David P., “Quantum Computers Aren’t Just Theoretical”, *Wall Street Journal*, (17 August 2000), p. B6.

[225] Console, Rodolfo and Nikolaev, Alexei (Eds.), Earthquakes Induced by Underground Nuclear Explosions (Springer-Verlag, Berlin, 1994).

[226] Anonymous, “In Brief – Stress Reducers”, *Bulletin of the Atomic Scientists*, 56, #3, 9 (May/June 2000).

[227] Finnearty, Brittnee, “Earthquake Control”, Geology 220 student project, Wittenberg University (2000). Available on the Internet at *http://www4.wittenberg.edu/academics/geol/progcrs/geol220/finneart/index.shtml*.

[228] Drexler, K. Eric, The Engines of Creation (Doubleday, New York NY, 1987).

[229] Drexler, K. Eric, Peterson, Chris, and Pergamit, Gayle, Unbounding the Future: The Nanotechnology Revolution (Foresight Institute, 1991). Available on the Internet at *http://www.foresight.org/UTF/Unbound_LBW/index.html*.

[230] Crandall, B. C.(Ed.), Nanotechnology (MIT Press, Cambridge MA, 1997).

[231] Piller, Michael and Wagner, Michael, "Evolution", Airdate: Week of 9-25-89, Episode 50 of *Star Trek: The Next Generation* (Paramount Pictures, Hollywood CA, 1989).

[232] Freitas, Robert A., Jr., Nanomedicine Volume I: Basic Capabilities (Landes Bioscience, Austin TX, 1999).

[233] Fujiwara, M. C. et al, "Resonant Formation of $d\mu t$ Molecules in Deuterium: An Atomic Beam Measurement of Muon Catalyzed *dt* Fusion", *Phys. Rev. Letts.*, 85, #8, 1642-1645 (21 August 2000).

[234] Morehouse, David, Psychic Warrior (St. Martin's Press, New York NY, 1996).

[235] Schnabel, Jim, Remote Viewers: The Secret History of America's Psychic Spies (Bantam Doubleday Dell Publishing, New York NY, 1997).

[236] Schevitz, Tanya, "U. S. Schools Fall Short of Tech Demands", *San Francisco Chronicle*, pp.A1, A5 (Monday, 9 October 2000).

[237] The Avalon Project, "Laws of War: Declaration of St. Petersburg; November 29, 1868", Yale Law School (1998). Available on the Internet at *http://www.yale.edu/lawweb/avalon/lawofwar/decpeter.htm*.

[238] The Avalon Project, "Laws of War: Declaration on the Use of Bullets Which Expand or Flatten Easily in the Human Body; July 29, 1899", Yale Law School (1998). Available on the Internet at *http://www.yale.edu/lawweb/avalon/lawofwar/dec99-03.htm*.

[239] The Avalon Project, "Laws of War: Declaration on the Use of Projectiles the Object of Which is the Diffusion of Asphyxiating or Deleterious Gases; July 29, 1899", Yale Law School (1998). Available on the Internet at *http://www.yale.edu/lawweb/avalon/lawofwar/dec99-02.htm*.

[240] The Avalon Project, "Laws of War: Opening of Hostilities (Hague III); October 18, 1907", Yale Law School (1998). Available on the Internet at *http://www.yale.edu/lawweb/avalon/lawofwar/hague03.htm*.

[241] The Avalon Project, "Laws of War: Restrictions With Regard to the Exercise of the Right of Capture in Naval War (Hague XI); October 18, 1907", Yale Law School (1998). Available on the Internet at *http://www.yale.edu/lawweb/avalon/lawofwar/hague11.htm*.

[242] The Avalon Project, "Laws of War: Laying of Automatic Submarine Contact Mines Hague VIII); October 18, 1907", Yale Law School (1998). Available on the Internet at *http://www.yale.edu/lawweb/avalon/lawofwar/hague08.htm*.

[243] Department of Defense, "CCW/APL: Certain Conventional Weapons/Anti-Personnel Landmines. Executive Summary" (undated). Available on the Internet at *http://www.acq.osd.mil/acic/treaties/ccwapl/ccw_es.htm*.

[244] Department of Defense, "Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which may be Deemed to be Excessively Injurious or to have Indiscriminate Effects" (undated). Available on the Internet at *http://www.acq.osd.mil/acic/treaties/ccwapl/ccw.htm*.

[245] Department of Defense, "Review Conference of the States Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which may be Deemed to be Excessively Injurious or to have Indiscriminate Effects" (undated). Available on the Internet at *http://www.acq.osd.mil/acic/treaties/ccwapl/ccw_2.htm*.

[246] International Committee of the Red Cross, "Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which may be Deemed to be Excessively Injurious or to have Indiscriminate Effects, Geneva, 10 October 1980. States which have adhered to the Convention and annexed Protocols" (26 September 2000). Available on the Internet at *http://www.icrc.org/eng/party_ccw*.

[247] Galvez, A., Maqueda, M., Martinez-Bueno, M., and Valdivia, E., "Scientific Publication Trends and the Developing World", *American Scientist*, 88, #6, 526-533 (November-December 2000).

[248] Harney, Robert C., "Information-Based Approach to Performance Estimation and Requirements Allocation in Multisensor Fusion for Target Recognition", *Optical Engineering*, 36, 789 (1997).

[249] Kuba, Tom, "Silent Sentry" Lockheed Martin Corporation (11 January 2000). Available on the Internet at *http://silentsentry.external.lmco.com/proj/nonsecure/sentry/SShome.htm*

[250] *Newsweek* (6 December 1999).

[251] Anonymous, Russia's Arms Catalog, Vol. 5, Air Defense (Military Parade Ltd., Moscow, 1997), pp. 231-233. Distributed by Zigzag Venture Group, 645 5th Avenue, New York NY 10022.

[252] Dagani, Ron, Jacoby, Mitch, Thayer, Ann M., and Schulz, William, "Nanotechnology: A Special Report", *Chemical & Engineering News*, 78, #42, 25-42 (16 October 2000).

[253] Sutcliffe, W.G., Condit, R. H., Mansfield, W. G., Myers, D. S., Layton, D. W., and Murphy, P. W., "A Perspective on the Dangers of Plutonium", Lawrence Livermore National Laboratory Report UCRL-JC-118825 (14 April 1995). Available on the Internet at *http://www.llnl.gov/csts/publications/sutcliffe/*.

[254] Alster, Jack, Iyer, S. and Sandus, O., "Molecular Architecture Versus Chemistry and Physics of Energetic Materials", in S. N. Balusu (Ed.), Chemistry and Physics of Energetic Materials (Kluwer Academic Publishers, Dordrecht NL, 1990), pp. 641-652.

[255] Rawls, Rebecca, "N_5^+ Cation Makes Explosive Debut", *Chemical & Engineering News*, 77, #4, 7 (25 January 1999).

[256] Foss, Christopher F., "China built 'Super Gun' to Gerald Bull design", *Jane's Defence Weekly*, 23, #5, 2 (4 February 1995).

[257] Foss, Christopher F., "China's new 'supergun' artillery could hit Taiwan from mainland", *Jane's Defence Weekly*, 32, #11, 5 (15 September 1999).

[258] Anonymous, "Range Classifications", Center for Defence & International Security Studies, Lancaster UK (undated). Available on the Internet at *http://www.cdiss.org/bmrange.htm*.

[259] Pike, John, "Ballistic Missile Basics", Federation of American Scientists (4 June 2000). Available on the Internet at *http://www.fas.org/nuke/intro/missile/basics.htm* .

[260] International Committee of the Red Cross, Blinding Weapons (ICRC, Geneva, 1990).

[261] Mumford, Michael D., Rose, Andrew M., and Goslin, David S., "An Evaluation of Remote Viewing Research and Applications", American Institutes for Research (29 September 1995). Available on the Internet at *http://www.parascope.com/en/articles/starGateReport.htm*.

INDEX

BIOGRAPHY OF AUTHOR

Dr. Harney has occupied the NAVSEA Chair of Total Ship Systems Engineering – Combat Systems at the Naval Postgraduate School (NPS) since 1995 and is a Senior Lecturer with the Institute for Defense Systems Engineering & Analysis. He has undergraduate degrees in chemistry and physics from Harvey Mudd College and a doctorate in Engineering-Applied Science from the University of California at Davis-Livermore. His prior service includes 25 years work on defense technologies and weapons systems of all kinds at national laboratories (Naval Research Laboratory, Lawrence Livermore National Laboratory, Los Alamos National Laboratory, MIT Lincoln Laboratory) and defense industry (Martin Marietta) in positions ranging from technical staff to senior project management. He has published over 70 technical publications, holds 5 patents, has chaired 5 international technical conferences, and taught over 50 short courses on lasers, laser radar, systems engineering, and combat systems design.

Areas of prior significant research include inertial confinement fusion, picosecond time resolution instrumentation, nonlinear optics, laser Raman spectroscopy, high energy lasers, explosive-pumped lasers, adaptive optical systems, atmospheric propagation and modeling, laser radar, electro-optical imaging systems, electronic warfare, air defense missile systems, simulation and modeling of sensor systems, multisensor fusion, weapons effects, proliferation of weapons of mass destruction (nuclear, chemical, biological, radiological), technology forecasting, systems engineering, and ship survivability. A significant part of his earlier work involved investigating the vulnerabilities of existing and proposed weapons systems. From 1997-2000 he was a participant in the NPS Area Denial study which provided the inspiration and information for this document.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center ………………………………………………...2
   8725 John J. Kingman Road, Suite 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library …………………………………………………………………..2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, CA 93943

3. Research Office Code 09 ………………………………………………………………2
   Naval Postgraduate School
   Monterey, CA 93943-5138

4. Superintendent Code 00 ………..…………………………………………………..1
   Naval Postgraduate School
   Monterey, CA 93943

6. Dr. Richard Elster …………………………………………………………………. 1
   Provost Code 01
   Naval Postgraduate School
   Monterey, CA 93943

7. Dr. Peter Purdue ……………………………………………………………………….1
   Associate Provost, Strategic Planning Code 012
   Naval Postgraduate School
   Monterey, CA 93943

8. Dr. Ken Euske ………………………………………………………………………….. 1
   Dean, Graduate School of Business and Public Policy Code 08
   Naval Postgraduate School
   Monterey, CA 93943

9. Dr. Rudy Panholzer ……………………………………………………………………1
   Dean, Graduate School of Engineering and Applied Science Code 07
   Naval Postgraduate School
   Monterey, CA 93943

10. Prof. Wayne Hughes, Jr. ….……………………………………………………………. 1
    Dean, Graduate School of Operational & Information Science Code 06
    Naval Postgraduate School
    Monterey, CA 93943

10. Institute for Defense Systems Engineering & Analysis ………………………………. 30
Naval Postgraduate School
Monterey, CA 93943

11. Dr. Robert C. Harney, Code PH/Ha …………………………………………………. 50
Institute for Defense Systems Engineering & Analysis
Naval Postgraduate School
Monterey, CA 93943

12. VADM Arthur K. Cebrowski ………………………………………………………….1
Director, Office of Force Transformation
Office of the Secretary of Defense
The Pentagon
Washington, DC 20301

13. VADM Dennis McGinn ……………………………………………………………..1
Deputy CNO for Warfare Requirements and Programs (N7)
The Pentagon
Washington, DC 20301

14. RADM Rodney P. Rempt ………………………………………………………. 1
President
Naval War College
686 Cushing Road
Newport, RI 02841

15. RADM Robert G. Sprigg …………………………………………..………………1
Commander
Navy Warfare Development Command
686 Cushing Road
Newport, RI 02841

16. Chief of Staff ……………………………………………………………………… 1
Navy Warfare Development Command
686 Cushing Road
Newport, RI 02841

17. Technical Director ………………………………………………………………… 5
Navy Warfare Development Command
686 Cushing Road
Newport, RI 02841

18. Red Cell Director …………………………………………………………………….1
Navy Warfare Development Command
686 Cushing Road
Newport, RI 02841

19. Director ……………………….………………………………………………………………1
Maritime Battle Center
Navy Warfare Development Command
686 Cushing Road
Newport, RI 02841

20. Department Head …………….………………………………………………………….. 1
Operations Department
Navy Warfare Development Command
686 Cushing Road
Newport, RI 02841

21. Department Head …………….………………………………………………………….. 1
Concepts Department
Navy Warfare Development Command
686 Cushing Road
Newport, RI 02841

22. Department Head …………….………………………………………………………….. 1
Doctrine Department
Navy Warfare Development Command
686 Cushing Road
Newport, RI 02841

23. Deputy Department Head ……………………………………………………………….. 1
Concepts Department
Navy Warfare Development Command
686 Cushing Road
Newport, RI 02841

24. Deputy Department Head ……………………………………………………………….. 1
Operations Department
Navy Warfare Development Command
686 Cushing Road
Newport, RI 02841

25. Deputy Director ……………………………………………………………………………..1
Maritime Battle Center
Navy Warfare Development Command
686 Cushing Road
Newport, RI 02841

26. Deputy Department Head ……………………………………………………………………..1
Doctrine Department
Navy Warfare Development Command
686 Cushing Road
Newport, RI 02841

27. ADM James Hogg, USN (Ret.) ……………………………………………………….. 10
Director, CNO Strategic Studies Group
686 Cushing Road
Newport, RI 02841

28. Mr. Hal Hultgren …………………………………………………………………… 1
Naval Undersea Warfare Center Code 601
Newport, RI 02841

29. Mr. Frank White …………………………………………………………………. 1
Space and Naval Warfare Systems Center Code D4402
53560 Hull Street
San Diego, CA 92152-5001

30. Mr. Ray E. Glass ……………………………………………………………………1
Space and Naval Warfare Systems Center Code D4402
53560 Hull Street
San Diego, CA 92152-5001

31. Dr. Richard Kass ……………………………………………………………………1
Analysis Division Chief
U. S. Joint Forces Command Joint Experimentation, J97
1562 Mitscher Ave., Suite 200
Norfolk, VA 23551-2488

32. Ms. Annette Ratzenberger ……………………………………………………………..1
U. S. Joint Forces Command Joint Experimentation, J97
1562 Mitscher Ave., Suite 200
Norfolk, VA 23551-2488

33. Mr. Vince Roske, Jr. ……………………………………………………………….. 1
The Joint Staff, J8
The Pentagon
Washington, DC 20318-8000

34. Center for Naval Analyses …………………………………………………………. 1
4401 Ford Avenue
Alexandria, VA 22302-0268

35. Dr. John Hanley ………………………………………………………………………… 1
Commander-in-Chief USCINCPAC/J00
Box 64031
Camp H. M. Smith, HI 96861-4031

36. Mr. Andrew Marshall ……………………………………………………………………. 2
Director of Net Assessment
Office of the Secretary of Defense
The Pentagon, Room 3A930
Washington, DC 20301

37. Dr. Michael Pillsbury ……………………………………………………………………. 1
Office of Net Assessment
Office of the Secretary of Defense
The Pentagon, Room 3A930
Washington, DC 20301

38. Jeffrey R. Cares ……………………………………………………………………………..1
31 Willow Street
Newport, RI 02840

39. Mr. Thomas J. Kelly ……………………………………………………………………. 1
Office of Naval Intelligence
Directorate of Intelligence
4251 Suitland Road
Washington, DC 20395-5720

40. Prof. Gordon Schacher …………………………………………………………….. 5
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

41. Prof. William Kemple …………………………………………………………………… 1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

42. Prof. Walter LaBerge ………………………………………………………………………..1
Institute for Defense Systems Engineering & Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

43. Prof. Phil Depoy ……………………………………………………………………………..1
Institute for Defense Systems Engineering & Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

44. Mr. Nelson Irvine 1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

45. Prof. Steven E. Pilnick 1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

46. Prof. Wayne P. Hughes, Jr. 1
Department of Operations Research
Naval Postgraduate School
Monterey, CA 93943-5101

47. Prof. Shelley Gallup 1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

48. Prof. Alex Callahan 1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

49. Mr. Curtis Blais 1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

50. Prof. Patrick Parker 1
Institute for Defense Systems Engineering & Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

51. Prof. Michael Sovereign 1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

52. Prof. Michael Melich 10
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

53. Prof. Rodney Johnson …………………………………………………………………….1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

54. Prof. John Osmundsen ……………………………………………………………………1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

55. Prof. D. C. Schleher ………………………………………………………………………1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

56. Prof. Xavier Maruyama …………………………………………………………………..1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93942-5101

57. Prof. John Arquilla ………………………………………………………………………..1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

58. Prof. Gordon McCormick ………………………………………………………………….. 1
Special Operations Academic Group
Naval Postgraduate School
Monterey, CA 93943-5101

59. Ms. Cathy Spencer ………………………………………………………………………. 1
Institute for Joint Warfare Analysis
Naval Postgraduate School
Monterey, CA 93943-5101

60. Prof. Charles N. Calvano …………………………………………………………………1
Department of Mechanical Engineering
Naval Postgraduate School
Monterey, CA 93943-5101

61. Prof. David W. Byers ……………………………………………………………………..1
Department of Mechanical Engineering
Naval Postgraduate School
Monterey, CA 93943-5101

62. Prof. Fotis Papoulias ……………………………………………………………………..1
Department of Mechanical Engineering
Naval Postgraduate School
Monterey, CA 93943-5101

63. Prof. Morris Driels …………………………………………………………………… 1
Department of Mechanical Engineering
Naval Postgraduate School
Monterey, CA 93943-5101

64. Prof. Matthew Kelleher ……………………………………………………………….. 1
Department of Mechanical Engineering
Naval Postgraduate School
Monterey, CA 93943-5101

65. Prof. John Ciezki …………………………………………………………………….. 1
Department of Electrical Engineering
Naval Postgraduate School
Monterey, CA 93943-5101

66. Prof. Jeffrey Knorr ……………………………………………………………………..1
Department of Electrical Engineering
Naval Postgraduate School
Monterey, CA 93943-5101

67. Prof. Conrad Newberry ……………………………………………………………….. 1
Department of Aeronautical Engineering
Naval Postgraduate School
Monterey, CA 93943-5101

68. Prof. William Maier ……………………………………………………………………1
Department of Physics
Naval Postgraduate School
Monterey, CA 93943-5101

69. Prof. William Colson …………………………………………………………………..1
Department of Physics
Naval Postgraduate School
Monterey, CA 93943-5101

70. Prof. Steven Baker ……………………………………………………………………. 1
Department of Physics
Naval Postgraduate School
Monterey, CA 93943-5101

71. Prof. Alfred Cooper 1
Department of Physics
Naval Postgraduate School
Monterey, CA 93943-5101

72. Prof. James Sanders 1
Department of Physics
Naval Postgraduate School
Monterey, CA 93943-5101

73. Prof. Chris Olsen 1
Department of Physics
Naval Postgraduate School
Monterey, CA 93943-5101

74. CAPT Fredrick Rocker 1
Department of National Security Affairs
Naval Postgraduate School
Monterey, CA 93943-5101

75. Prof. Edward Olsen 1
Department of National Security Affairs
Naval Postgraduate School
Monterey, CA 93943-5101

76. Prof. Glen Browder 1
Department of National Security Affairs
Naval Postgraduate School
Monterey, CA 93943-5101

77. Prof. James Wirtz 1
Department of National Security Affairs
Naval Postgraduate School
Monterey, CA 93943-5101

78. Prof. Peter Lavoy 1
Department of National Security Affairs
Naval Postgraduate School
Monterey, CA 93943-5101

79. Prof. Raymond E. Franck 1
Department of Systems Management
Naval Postgraduate School
Monterey, CA 93943-5101

80. Prof. Paul McCarthy ……………………………………………………………………. 1
Department of Systems Management
Naval Postgraduate School
Monterey, CA 93943-5101

81. Prof. Orin Marvel ……………………..…………………………………………… 1
C4I Academic Group
Naval Postgraduate School
Monterey, CA 93943-5101

82. Prof. Bard Mansager …………………………………………………………….. 1
Department of Mathematics
Naval Postgraduate School
Monterey, CA 93943-5101

83. Prof. David Schrady ………………………………………………………………1
Department of Operations Research
Naval Postgraduate School
Monterey, CA 93943-5101

84. Prof. Donald Gaver ……………………………………………………………… 1
Department of Operations Research
Naval Postgraduate School
Monterey, CA 93943-5101

85. Prof. Patricia Jacobs ………………………………………………………………1
Department of Operations Research
Naval Postgraduate School
Monterey, CA 93943-5101

86. Prof. James Eagle …………………………………………………………………1
Department of Operations Research
Naval Postgraduate School
Monterey, CA 93943-5101

87. Prof. Tom Hoivik …………………………………………………………………1
Department of Operations Research
Naval Postgraduate School
Monterey, CA 93943-5101

88. CDR W.T. McCoy………………………………………………………………. 1
Curriculum Officer Code 34
Naval Postgraduate School
Monterey, CA 93943-5101

89. CDR Mark Rhoades ………………………………………………………………………. 1
Curriculum Officer Code 31
Naval Postgraduate School
Monterey, CA 93943-5101

90. Prof. David Olwell……………………………………………………………………….. 1
Operations Research Department
Naval Postgraduate School
Monterey, CA 93943-5101

91. Prof. Alan Washburn…………………………………………………………………….. 1
Operations Research Department
Naval Postgraduate School
Monterey, CA 93943-5101

92. CDR Matt Boensel……………………………………………………………………….. 1
Operations Research Department
Naval Postgraduate School
Monterey, CA 93943-5101

93. CDR David Spain ……………………………………………………………………….. 1
N3/N5 Chair of Strategic Planning
Naval Postgraduate School
Monterey, CA 93943-5101

94. LT Raymond Buettner ……………………………………………………………………1
Information Warfare Curriculum
Naval Postgraduate School
Monterey, CA 93943-5101

95. Rex Buddenberg ……………………………………………………………………….. 1
Information Systems Department
Naval Postgraduate School
Monterey, CA 93943-5101

Naval Postgraduate School
Monterey, California